NCSC-TG-031
Version 1
ISWG-9608-28

National Computer Security Center

Certification and Accreditation Process Handbook for Certifiers

July 1996

Approved for Public Release:
Distribution Unlimited

NCSC-TG-031
Library No. S-240,999
Version 1

FOREWORD

The National Computer Security Center is publishing the *Certification and Accreditation Process Handbook for Certifiers* as part of the "Rainbow Series" of documents. This document continues a subseries on certification and accreditation (C&A) and provides the certifier and Accreditor with a structured process by which to perform a C&A of a system. It should be viewed as guidance in determining the amount of effort and the resources necessary to certify and accredit a system. As technology that supports the infrastructure of automated systems becomes more sophisticated, the C&A process will, no doubt, require new or additional guidance. However this document provides the necessary C&A guidance for now and into the near future.

The terminology and structure in the *Certification and Accreditation Process Handbook for Certifiers* has been harmonized with the on-going *DoD Information Technology Security Certification and Accreditation Process* (DITSCAP). Thus DoD elements may use this document in support of their C&A requirements. However the document is not DoD specific. The C&A process described is consistent with the one in the earlier guideline, *Introduction to Certification and Accreditation*. Non DoD agencies and organizations should have little problems in seeing the parallels and using this latest document in their C&A programs.

I invite your suggestions for revising this document. We plan to review and revise this document as the need arises. Please address all proposals for revision through appropriate channels to:

Defense Information Systems Agency
701 South Courthouse Road
Arlington, VA 22204-2199
Attention: Center for Information Systems Security

July 1996

John C. Davis
Director
National Computer Security Center

DEDICATION

This document is dedicated to Barbara L. Valeri who as Director for Information Systems Security at OSD strongly supported a comprehensive C&A program for the DoD and the federal Government. Her emphasis on the development of aids for those engaged in the C&A process facilitated greatly the final review and publication of this document.

ACKNOWLEDGMENT

The initial version of this document was produced under the leadership of Lieutenant Commander Candice Stark and Major Bill Fetech while at NSA. The final revision was accomplished under the NSA/CISS partnership of Paul Wisniewski, NSA, and Jack Eller, DISA/CISS with the help of Mark Havelin, NSA, Joel Sachs of Sachs Group, Dennis Winchell of Logicon, and Barry Stauffer of CORBETT Technologies.

ABSTRACT

The Certification and Accreditation Process Handbook for Certifiers establishes a standard approach for performing C&A by providing guidance on the C&A activities and the associated level of effort required based on assurance requirements and other tailoring factors related to the system. Assurance is defined as a measure of confidence that the security features, attributes, and functions enforce the security policy. Assurance can be established for operations (enterprises), systems, operational environments, and components or mechanisms. Assurance refers to the claims and evidence for believing the correctness, effectiveness, and workmanship of the security service or mechanism. Certification verifies and validates the security assurance for a system associated with an environment. Accreditation evaluates whether the operational impacts associated with any residual system weaknesses are tolerable or unacceptable. Life-cycle assurance requirements provide a framework for secure system design, implementation, and maintenance.

Suggested Keywords: accreditation, Accreditor, accountability, assurance, availability, computer security, confidentiality, certification, certifier, DAA, information security, information systems security, INFOSEC, integrity, threat, and vulnerability

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

LIST OF TABLES

SECTION 1

INTRODUCTION

1.1 Background

In the present environment of declining resources and because of the rapid advances in systems and technology, current U.S. Government security policies do not provide sufficient detailed guidance on how to certify and accredit a system. A system is a collection of components that may include computer hardware, firmware, software, data, procedures, environment, and people, so related as to behave as an interacting or interdependent unit to perform a mission [1]. These components should be under a single operational and administrative control to provide focused oversight and responsibility.

This lack of guidance has led agencies in the Federal community to develop separate methodologies that may or may not provide detailed guidance needed to analyze systems from an information systems security (INFOSEC) perspective. INFOSEC relates to the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit. INFOSEC also includes protection against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats [2].

National policy for the security of national security telecommunications and information systems provides initial objectives, policies, and an organizational structure to guide the conduct of activities directed toward safe-guarding systems that process national security information [1]. To ensure national policy is enforced effectively and consistently, methodologies and tools need to be developed to support the certification and accreditation (C&A) process. Today's challenge is to be able to comply with national policy in support of a cost-effective and efficient C&A process without jeopardizing the protection mechanisms, practices, and security safeguards of Federal systems. This handbook has been designed to meet the Federal Security policies including OMB A-130. A list of Federal Security policies can be found in [1].

1.2 Purpose

The purpose of this handbook is to establish a standard approach for performing C&A on systems regardless of the acquisition strategy or life-cycle status. Certification is the comprehensive assessment of the technical and nontechnical security features and other safeguards of a system associated with its use and environment to establish the extent to which a particular system meets a set of specified security requirements. Certification is in support of accreditation. Certification is an integral part of risk management and should be continually reviewed and updated throughout the system life-cycle. The Certification Phase of the C&A process includes a system analysis to identify weaknesses in operating the system with specified counter-measures in a particular environment, as well as an analysis of the potential vulnerabilities of these weaknesses. Planning for accreditation should be implemented at the beginning of the system life-cycle to ensure that security protection mechanisms and safeguards are designed and integrated into the system and/or subsystems, that security decisions are not delayed leading to costly retrofits and delays in operationally fielding the system, and that adequate resources are provided for C&A activities.

Accreditation is the formal declaration by the Designated Approving Authority (DAA) that an automated information system (AIS) is approved to operate in a particular security mode using a prescribed set of safeguards [1] and should be strongly based on the residual risks identified during certification. The Accreditor[1] has the formal responsibility in authorizing operation of the system. Since the risk to a system changes over the life of the system, the Accreditor must remain actively involved in the accreditation/reaccreditation process during the entire system life-cycle. The level of risk the Accreditor is willing to accept should be based upon the degrees of assurance.

This handbook provides guidance about the C&A process based on the degrees of assurance required and other factors related to a system. Assurance is the measure of confidence that the security features, attributes, and functions enforce the security policy. Assurance can be established for operations (enterprises), systems, operational environments, and components or mechanisms. Assurance refers to the claims and evidence for believing the correctness, effectiveness, and workmanship of the security service or mechanism. Certification verifies and validates the security assurance for a system associated with an environment. Accreditation evaluates whether the operational impacts associated with any residual system weaknesses are tolerable or unacceptable. Life-cycle assurance requirements provide a framework for secure system design, implementation, and maintenance. The degrees of assurance assumed by a development team, certification team, or Accreditor about a system reflect the confidence that the system is able to enforce its security policy correctly during use and in the face of attacks [1].

The C&A process allows the DAA, Program Manager, and User Representative to tailor the certification efforts to the particular system mission, threats, environment, degrees of assurance, and criticality of the system, as necessary, as long as they comply with network connection rules. With a standard approach established, reuse of both the technical and nontechnical analyses from the certification effort for recertification or certification of a similar system might be possible. The C&A process should encourage and preserve commonality in understanding, be consistent in application, be

[1] The term DAA and Accreditor are used synonymously and the terms Certification Authority (CA) and Certifier will be used synonymously throughout this document. The term Program Manager will be used throughout this document to refer to the person responsible for the system. This person is generally the acquisition organization■s program manager during the acquisition, the system program manager during operation of the system or the maintenance organization's project manager when a system is undergoing a major change.

open to evolution and growth, employ feedback, and be applied continuously [3]. This process should be scalable to the size of the system, repeatable, and predictable.

1.3 Scope

This handbook is for the use of all personnel involved in the C&A of systems regardless of the classification or sensitivity of the system. This handbook advocates degrees of assurance as the initial basis for determining the level of effort necessary to complete the C&A. Once the degrees of assurance have been determined, the certification team can then identify the level-of-effort required for certification of the system. This handbook is intended to assist the certification team members in determining and applying the applicable tailoring factors to their system. This handbook is part of a series of documents on C&A with which the certification team members should become familiar to perform an appropriate type of certification. Appendix A contains abstracts of the other documents in this series.

1.4 Document Organization

This document defines a four-phased approach to C&A. Chapter 2 describes the C&A process. Activities are specified along with their respective input and output. Chapters 3 through 6 present the four phases. Chapter 3 addresses the Pre-Certification Phase (Phase I) and also provides guidance in analyzing the system requirements and identifying the appropriate tailoring factors. Chapter 4 addresses the Certification Phase (Phase II), discussing the detailed activities in analyzing the system. Chapter 5 delineates the activities of the Accreditation Phase (Phase III). Chapter 6 explains the Post-Accreditation Phase (Phase IV).

SECTION 2

C&A PROCESS

The C&A process consists of four interrelated phases with feedback to previous phases as necessary. Each phase may require one or more activities. Each activity lists several tasks that may need to be performed depending on various factors that will be discussed below. Each task involves both input and output. The input represents information that is needed to complete the task. The output represents the products or information resulting from completion of the task and may be used as input to subsequent activities. For example, to understand the system's security requirements, the certification team needs to review the mission of the system (an input), ensuring that the security requirements have been documented and validated. Appendix B contains a detailed list of the tasks, input, and output of each task and Chapters 3 through 6 provide specific information on the use of this input and output. For a glossary of terms, policies, and definitions, refer to [1].

The C&A process is expanded in this document to (1) provide more detail concerning each phase of the process, particularly the Certification Phase; and (2) ensure that the individuals who have C&A responsibilities understand the role of the certification team. Figure 2-1 illustrates the C&A process. Some of the tailoring factors considered in the C&A process include:

- System requirements
- Degrees of assurance
- Programmatic considerations
- System complexity
- Security environment
- Risk-related considerations (e.g., mode of operation, highest level of data processed by the system, user capabilities, threats, vulnerabilities)
- Available documentation (e.g., certification or evaluation evidence)

👍 Accreditation considerations

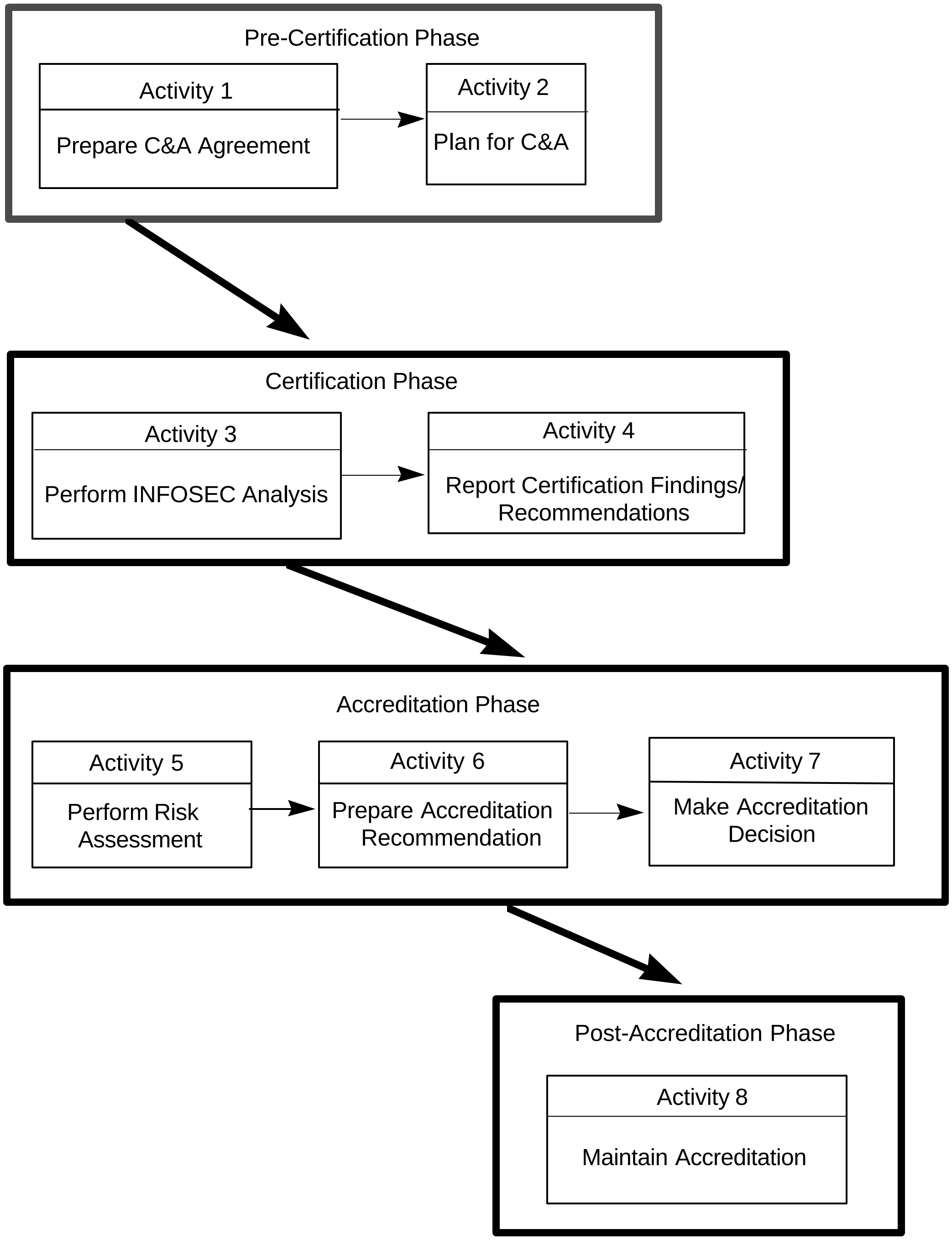

Pre-Certification Phase
Activity 1
Prepare C&A Agreement
Activity 2
Plan for C&A
Certification Phase
Activity 3
Perform INFOSEC Analysis
Activity 4
Report Certification Findings/ Recommendations
Accreditation Phase
Activity 5
Perform Risk Assessment
Activity 6
Prepare Accreditation Recommendation
Activity 7
Make Accreditation Decision
Post-Accreditation Phase
Activity 8
Maintain Accreditation

Figure 2-1 C&A Process

2.1 Phase I: Pre-Certification

Phase I includes two activities: (1) prepare C&A agreement, and (2) plan for C&A. This phase involves gathering data about the system to analyze the tailoring factors and ensuring that the Accreditor and the certification team members understand their responsibilities for the effort.

2.1.1 Activity I - Prepare C&A Agreement

The purpose of Activity l is to analyze and document system-specific information that impacts the C&A effort and document the results in the C&A Agreement. Activity 1 tasks are critical to determining the appropriate C&A tailoring factors to be used throughout the C&A process and are discussed in detail in Chapter 3. The tasks are:

- Analyze needs
- Determine usage requirements that impact C&A (e.g., operational requirements and procedures related to security)
- Analyze risk-related considerations
- Determine certification type
- Identify C&A team
- Prepare the C&A Agreement

The certification team documents the results of the system requirements analysis and tailoring in the C&A Agreement which is submitted to the DAA, Program Manager, and the User's Representative for approval.

2.1.2 Activity 2 - Plan for C&A

The threefold purpose of Activity 2 is to plan the C&A effort, obtain agreement on the C&A approach and level-of-effort, and to identify and obtain the necessary resources. C&A planning tasks are based on the information collected during Activity 1 and are also discussed in detail in Chapter 3. The tasks include:

- Identify secondary factors
- Determine applicability of documentation
- Develop C&A plan
- Obtain approval of the C&A plan.

2.2 Phase II: Certification

Phase II includes two Activities: (1) perform INFOSEC analysis and (2) report certification findings and recommendations. Both the analysis and the findings/recommendations depend on the tailoring factors identified in the previous phase. Phase II also helps the certification team analyze the potential vulnerabilities that may exist. The areas of vulnerability that the certification team should focus on include (1) the protection of information from unauthorized access - confidentiality; (2) denial of service - availability; (3) the integrity of the system and data - integrity; and (4) the ability to ensure that system events are traceable to persons or processes who may then be held responsible for their actions - accountability. (Accountability includes both authenticity and non-repudiation.)

2.2.1 Activity 3 - Perform INFOSEC Analysis

The purpose of Activity 3 is to analyze INFOSEC threats, vulnerabilities, countermeasures, and associated risks. This Activity includes the analysis and testing from the various security disciplines (e.g., computer security (COMPUSEC), communications security (COMSEC), physical security, TEMPEST with an integrated INFOSEC perspective, as well as the results from applicable product evaluations, system or product profiles, and/or certifications. It does not include validating the security requirements of the system described in the statement of work (SOW), security policy, or system specification. Activity 3 is discussed in detail in Chapter 4. The tasks are:

- Analyze detailed system information
- Conduct INFOSEC analysis (e.g., documentation review, testing, architecture studies)
- Conduct vulnerability assessment and risk analysis

2.2.2 Activity 4 - Report Certification Findings/Recommendations

The purpose of Activity 4 is to completely document the certification results in a certification package. This is the consolidation of all the certification analysis, testing, and findings.

2.3 Phase III: Accreditation

Phase III involves three activities: (1) perform risk assessment including an optional accreditation visit to the operational site(s), (2) report findings and recommendations, and (3) make the accreditation decision. This decision is based on the recommendation from the Certification Authority (CA), which is derived from the documentation gathered by the certification team, the testing conducted, and mission considerations. At this point in the process, the CA has completed his/her function and should not be involved in the accreditation decision.

2.3.1 Activity 5 - Perform Risk Assessment

The purpose of Activity 5 is to review the analysis, documentation, vulnerabilities, and residual risks to support the accreditation decision to be made by the Accreditor. The Accreditor or his/her representative(s) may conduct a site accreditation survey. This survey should be used to verify that the residual risks are at an acceptable level and to validate the contents of the C&A packages. For systems that are developed for multiple locations, the Accreditor's staff may need to perform some of the tasks required in Activity 3 (e.g., TEMPEST, COMSEC, contingency plan testing, physical security analysis, and operational security review). The tasks include:

- An optional site survey
- Assess vulnerabilities and associated risk
- Residual risk identification

2.3.2 Activity 6 - Prepare Accreditation Recommendation

The purpose of Activity 6 is to prepare the accreditation recommendation and document all the results of previous analyses.

- Make accreditation recommendation
- Complete accreditation package.

2.3.3 Activity 7 - Make Accreditation Decision

The Accreditor makes the decision on whether to approve the operation of the system under certain conditions, in a specified environment, and accepts the residual risk. The Accreditor is involved throughout the prior phases so an informed accreditation decision can be made. This Activity is discussed in detail in Chapter 5. The tasks include:

- Determine decision to operate

2.4 Phase IV: Post-Accreditation

Phase IV involves one Activity, which is to maintain the security posture and the accreditation of the system. To ensure the accreditation is properly maintained, the Accreditor is encouraged to perform periodic compliance inspections throughout the life of the system and recertify/reaccredit the system when required. To ensure the accreditation is maintained, a configuration or change management system must be implemented and procedures established for baselining, controlling, and monitoring changes to the system.

2.4.1 Activity 8 - Maintain Accreditation

Activity 8 of the process is an ongoing activity throughout the system life-cycle. Accreditation maintenance involves ensuring that the system continues to operate within the stated parameters as specified in the accreditation letter. Any substantial changes to the stated parameters of the accreditation may require that the system be recertified and reaccredited. Additionally, periodic reaccreditation is required due to both regulatory/policy requirements and changes that occur to the system. Maximum reuse of previous evaluations and/or certifications is emphasized to expedite this phase. This Activity is discussed in detail in Chapter 6. The tasks include:

- Review system modifications

- Review vulnerabilities and threats

- Repeat process with Activity 3

SECTION 3

PHASE I: PRE-CERTIFICATION

This phase is divided into two activities. The first activity is to prepare the C&A Agreement (Section 3.1). When analyzing the system requirements, the CA should analyze the customer needs, determine usage requirements (e.g., security policy) that impact C&A, analyze risk-related considerations, and determine the certification type. The second activity is to plan for C&A (Section 3.2).

The degrees of assurance required for the system drive the amount of security analysis and testing required prior to certification. The degrees of assurance depend on the degree of importance placed upon four factors: availability, confidently, accountability, and integrity.

These four factors are the key security policy objectives common to all information systems and are defined as follows:

- Availability: The property of being accessible and usable upon demand by an authorized user [1].

- Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [1].

- Accountability: The property that allows the ability to identify, verify, and trace system entities as well as changes in status. Accountability is considered to include authenticity and nonrepudiation:

    - Authenticity: Security services designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information [2].

    - Nonrepudiation: Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data [2].

- Integrity: The property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

- Data Integrity: The attribute of data relating to the preservation of (1) its meaning and completeness; (2) the consistency of its representation(s); and (3) its correspondence to what it represents [1].

- System Integrity: The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system [1].

3.1 Activity I - Prepare the C&A Agreement

As stated in Chapter 2, the purpose of this activity is to analyze system specific information (i.e., tailoring factors) that impact the C&A effort and to prepare the C&A Agreement. It involves determining the appropriate C&A tailoring factors to be used throughout the C&A process.

3.1.1 Determine Responsibilities and Analyze Needs

The first activities in the Pre-Certification Phase is to analyze needs and to identify accreditation considerations. The CA should receive a request for certification assistance. When certification assistance is requested, a decision from the CAs management must be made concerning the commitment of resources (e.g., time, personnel) to the project. Without this initial commitment, the CA cannot begin to support the certification of the system.

3.1.1.1 Identify Accreditor and Other Important Individuals

The Designated Approving Authority "(DAA - Accreditor)" - Official with authority to formally assume responsibility for operating an AIS or network at an acceptable level of risk. [2] The Accreditor will require proof that the residual risks were properly identified and documented. The CA will take guidance and direction from the Accreditor. Consequently, the Accreditor must be identified as soon as possible. If the Accreditor has not been determined, the CA should request the operating agency to identify the Accreditor. Although the CA may begin gathering documentation about the system without the Accreditor identified, planning for and performing the certification should not proceed without indication and involvement of the Accreditor.

Other important security individuals with which the CA should become acquainted include, but are not limited to, the Program Managers (PM), security manager (sometimes called the Information Systems Security Manager (ISSM), and the Information Systems Security Officer (ISSO).

Federal/agency policies and regulations may contain additional information in this area and [1] contains a sample of these policies.

3.1.1.2 Determine System Responsibility

The organization and manager responsible for the system must be determined. As a system progresses through the life-cycle phases, system responsibility (engineering and management) may change. During acquisition, this responsibility may be the acquisition organization who will be represented by the system's PM. During the Operations and Maintenance phase of the system, this responsibility may be the System Manager or in the case of a major upgrade, the maintenance organization who will be represented by the upgrade Project Manager. (Throughout document the term PM (PM will be used to refer to the manager currently responsible for the system.) The CA should be aware that the system PM and the system User Representative, discussed in a subsequent section, may not be the same individuals or agencies. For the certification effort, the CA should work closely with the PM as the system progresses through various life-cycle phases. If the Accreditor determines that the system fails to meet the stated security requirements, the organization responsible for funding the needed changes must be determined and a plan developed for implementing those changes.

3.1.1.3 Determine Data Sensitivity

Being knowledgeable of the sources responsible for the various data elements will assist the CA in identifying any special requirements for protecting the information processed by the system. Although a system should have only one PM, the data that resides on or is processed by, the system might belong to many organizations. The definition of responsible data source is the agency/organization that can modify (append, change, delete) or allow other agencies to modify the individual data elements.[1] To assist the CA in identifying all the sensitivity levels of the data, Appendix D has been provided and cites basic categories of data sensitivity. The responsible data sources should provide the CA with the guidelines used to classify or to determine the sensitivity of their data. Once the analysis of the data has been completed, the highest data classification level may be determined.

3.1.1.4 Identify Users

The system users and maintenance personnel need to be identified and their roles understood. The term users refers to both the individuals who will actually interact with the system alone with individuals who may only receive products (e.g., listings, tapes, disks) produced by the system and will

[1] Responsible data source does not necessarily mean original data source.

not interact with the system. For DoD systems, the clearance levels of the users and the previously identified data classification/sensitivity will be used to help determine the risk index. For additional guidance on determining the risk index, [5] may be used.

Roles, responsibilities, and associated system capabilities must be identified for each user. These roles, responsibilities, and capabilities can be used by the CA to determine if the procedures and mechanisms are in place to allow the appropriate access authorizations (e.g., write, read, modify, delete). The user capabilities and clearance levels are major factors in determining the degrees of assurance for the various categories. Throughout the C&A process, the interests of the users may be vested in a User Representative.

The system users may be part of a single organization or a huge diverse community. The interface to the user community is through a "User Representative" who will represent the interests of the users in all C&A issues. The User Representative should provide the common voice in identifying the users roles, responsibilities, and capabilities. The User Representative should, at minimum, review and approve the security requirements, assurance factors, certification results, and any proposed security features.

3.1.1.5 Understand Environmental Requirements

Next, the environmental considerations (e.g., physical, mobility) that require additional security measures need to be identified and clearly understood. The emphasis should focus on the location of the operational system. Any change to the mobility requirements and specified environments may require the system to be recertified and reaccredited. All system and environment-related changes must be analyzed for their security impact. If the system (e.g., workstations, terminals, servers, mainframes/minicomputers) operates at a fixed location, then the specific environmental considerations (e.g., power, heating/ventilation/air conditioning (HVAC), physical security) can be clearly stated. Emphasis should not be placed on the environment of the development and maintenance locations as this is addressed in the configuration management plan covered in Chapter 4.

Since it is difficult to certify and accredit a mobile system at all possible locations, mobility requirements will impact the type and level of effort of the certification. The Accreditor may have to "type accredit", also called generic accreditation, the system for a generic environment. Type accreditation is the official authorization by the Accreditor to employ a system in a specified environment. It includes a statement of residual risk, delineates the operating environment and identifies specific use, operational constraints, and/or procedural workarounds. It may be performed when multiple platforms will be fielded in similar environments [1].

In this case the Accreditor would include a statement with the accreditation, such as, "This system is supplied with a generic accreditation. With the generic accreditation, the operators must take responsibility to monitor the environment for compliance with the environment as described in the accreditation documentation".

3.1.1.6 Understanding System and Functional Requirements

In parallel with understanding the environmental requirements, the system and functional requirements need to be identified. The CA should obtain documentation describing how and where the system will be used; the operational context in which the system will be used; the operation or enterprise the system leverages; and the users, functions, and mission of this operation. This information is often contained in the Concept of Operations (CONOPS) document. The CA should review and understand the security requirements, from all the above perspectives, to best resolve the appropriate system security requirements. From a security aspect, the CA should closely examine systems that are used both for support (training, exercises, developmental testing) and operations. The possibility of test or exercise data affecting the operational system, or visa versa, may be a serious problem and precautions should be implemented. The system architecture must not only support functional and performance requirements, but also the security requirements.

The CA should focus its efforts on obtaining the system security documentation that will be analyzed in Phase II. After the completion of this activity, the certification team can determine if additional system documentation will be needed. Team members should focus their analysis on the completeness and adequacy of the security documentation to support the C&A activities. If complete and adequate documentation is not available, the DAA, PM, and User Representative[1] will need to determine if it is cost-effective to produce the needed documents or accept the residual risk of not having them. This security documentation should consist of the following:

- SOW
- CONOPS
- Security Policy

3.1.1.7 Determine Accreditation Boundary

For the CA to scope the certification effort, a boundary must be defined such that everything inside that boundary is what will be accredited. Additionally, all connections and equipment outside the

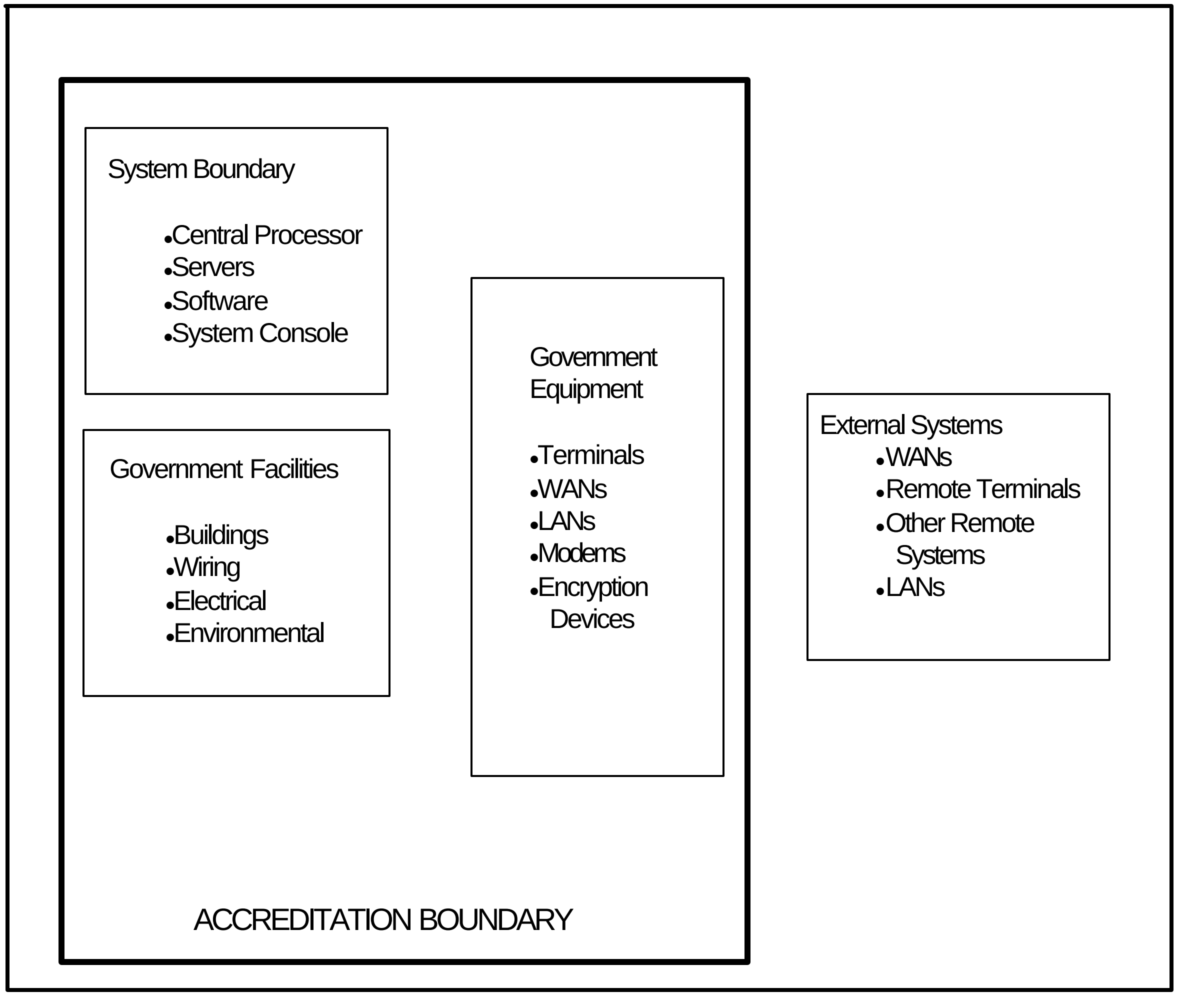
[1] It is recognized these managers may choose to designate someone to represent them at various reviews in the C&A process. Unless noted otherwise, the terms Accreditor, PM, and User Representative will be used to mean the principle or their designated representative.

boundary will require a Memorandum of Agreement (MOA) before connection to the system is allowed. Included inside the accreditation boundary may be a system boundary. The system boundary may be the equipment (e.g., hardware, software, interfaces) that is being acquired or instated. The accreditation boundary includes the system boundary, plus all other Government-furnished equipment (e.g., terminals, wide area networks (WANs), local wiring, local area networks (LANs), modems). A good rule to use in determining the accreditation boundary is that the Accreditor should have some type of configuration control over the equipment inside the boundary. The Accreditor must approve all changes to the system before their installation. The accreditation boundary should be as large as possible to preclude separate certifications and accreditations of individual systems and lessen the number of MOAs between separately accredited systems. Figure 3-1 depicts this concept.

While it is necessary to determine the specific accreditation boundary to focus and scope the C&A effort, all participants in the C&A process must consider the potential security impact of the system operations on the Defense Information Infrastructure (DII) and vice versa.

Figure 3-1 Accreditation Boundary

3.1.1.8 Identify and Examine External Connections



Since many systems are networked to other systems, the system integrator must be identified along with the Accreditor and ISSO(s) of the other systems. The CA should obtain the C&A evidence from these various end systems. If the end systems have not been certified and accredited, the Accreditor must be apprised of this fact along with the risk of connecting to these end systems. The system integrator may also be the organization responsible for the various phases of testing. Not only must the certification team be aware of external systems, but also the networks to which these external systems are connected. With fewer and fewer stand-alone systems being implemented and the increased use of automated guards to interconnect networks of various sensitivities and classifications, the degree of assurance placed on these guards increases dramatically.

The system CONOPS and systems level interface documents (Interface Requirements Specification and Interface Design Document) should be examined to identify all the connections and interfaces intended for the system. All external interfaces need to be carefully examined. The examination should first define the security constraints imposed on the system by the external connections, i.e., how do we protect this system. Secondly, the examination should define those constraints with which the system must comply to connect to other systems, i.e., how is the network protected. In examination of these interfaces, it is useful to view the type of interface. These types of interfaces include the following:

- Benign: A system that is not related to any other system is a benign system. Benign systems are closed communities without physical connection or local relationship to any other systems. Benign systems are operated exclusively of one another and do not share users, information, and/or processing with other systems.

- Passive: A system that is related indirectly to other systems is passive. Passive systems may or may not have a physical connection to other systems and their logical connection is controlled tightly. Stand-alone systems that pass information to other systems via magnetic media are passive. Systems that are physically connected but only receive information are passive.

- Active: A system that is connected directly to one or more other systems is active. Active systems are connected physically and have a logical relationship to other systems. Active systems permit users or processes to use multiple system resources freely. They allow users to alter data or provide limited restrictions to system resources across multiple systems.

3.1.1.9 Understand Network Connection Rules

The connection of an information system to a network requires that a particular system will not adversely affect the network's security posture. Connection also requires that the network will not adversely affect the system's own security posture. Connection rules should be defined for each interface identified in the previous section. Rules should be defined for both sides of each connection. The connection rules need to be clearly documented along with the progress for external systems to obtain connections to this system.

When connecting to another system or network that is outside the accreditation boundary, rules and procedures must be established and enforced to ensure that the security of the system and the interfacing network are properly maintained. These rules may be part of the security policy, CONOPS, or a separate document, but must be consistently applied and enforced for all connections. Each approved connection should be documented in an MOA between the Accreditors of the two systems.

3.1.2 Determine Usage Requirements that Impact C&A

3.1.2.1 Review Security Policies

The C&A activities should begin with examination of existing security policies associated with the system. Security policies can be established at different levels of abstraction. These levels focus on the entire operation or enterprise, the operational use or dependence on the system, the operational environment in which the system operates, and the system itself. In some cases the levels will be delineated and possibly, distinct; in others, they may be merged or combined into one policy. These levels of abstraction include:

- System Security Policy objective
- Organizational Security Policy
- Security requirements (technical security features, operational security features)

The security policy is the set of laws, rules, and practices that regulate how sensitive or critical information is managed, protected and distributed [1]. Assurance establishes the confidence that when a security policy is enforced, its associated security objectives, laws, rules, and practices are realized. It should include the types of use and access to be regulated within and across the accreditation boundary. Security policies are often organized into the area of confidentiality, integrity, availability, and accountability.

The organizational security policy focuses on the entire operation or enterprise. It contains high-level goals and objectives for the organization to perform its mission within acceptable risks. The operational security policy focuses on functions the organization performs, the elements and individuals that perform them, and the organization's reliance on an information system to leverage these functions. (The operational security policy is often included or embodied in the Security CONOPS.) The environmental security policy reflects the laws, rules, and practices that are intended to be enforced by the environment in which the system operates.

The system security policy reflects the set of laws, rules, and practices that are intended to be enforced by the system. The certification focuses on verifying and validating that the system architecture, design, and implementation enforce the system security policy through the system mechanisms. Reference [15] provides guidance for developing a security policy.

In reviewing the security policies, the CA should determine that they clearly state the basis for the policy objectives (e.g., Director of Central Intelligence Directive (DCID) 1/16, Office of Management and Budget (OMB) A-130) and applicable local policies and regulations. The CA must not review the security policy, CONOPS, and architecture in isolation, but should include the PM (with representatives from the developer/maintainer), the Accreditor, and the User Representative. However, the CA should have full unencumbered access to any documents or material in his/her work in reviewing security policies.

3.1.2.2 Understanding System Criticality

Criticality is a driving factor in determining the degrees of assurance [1]. Factors to consider in understanding criticality that will impact the degrees of assurance are (1) loss of life, or injury from system failure; (2) inability to perform the organization's responsibility due to system failure; (3) availability of manual backup systems to perform the organization's job if the system fails; (4) damage to resources; (5) damage to reputations; and (6) damage to national security. A good source for some of this information might be the Mission Need Statement (also called Statement of Need), Mission Impact Statement, Operational Requirements Document, the System Security Policy, CONOPS, or the purpose statement of the using organization.

To understand the system criticality and requirements, the CA should gain a perspective from at least the PM, User Representative, Accreditor, and ISSO. Should any conflicts arise in the definition or understanding of the security requirements, these conflicts should be referred to the PM, Accreditor, and User Representative for resolution. Once the high-level security requirements and system criticality have been understood and any conflicts resolved, identifying the systematical requirements/components should be less complicated. Additional guidance on determining a system's criticality can be found in [7, 8, 9, 10].

3.1.3 Analyze Risk-related Considerations

A threat is defined as the capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or an information system [2]. Threat may also some from intentional or accidental misuse by authorized users. At this point in the certification effort, the CA only needs a basic understanding of the threats to the system. In most cases, generic threat information is available and should be obtained. This information should be analyzed against customer perceived threats and a new threat analysis requested if necessary. Most systems have common threats such as attack by hackers, damage by disgruntled employees, and failure to follow standard procedure. Recent security surveys report that over 80% of the detected and reported attacks to computer systems are from inside the organization. This percentage breaks down into 24% due to inattention to procedures (carelessness), 26% due to inadequate training, and 30% due to dishonest employees [11]. Unfortunately, inappropriately and improperly increasing the amount of security on the system may not significantly decrease the insider threat. The CA should take into consideration the communication paths used, local processing capabilities, and the capabilities given to the users of the system. These common threats should always be analyzed and appropriate safeguards implemented.

In addition to threats from individuals or groups, the CA should consider threats from natural occurrences (e.g., hurricanes, earthquakes, floods, lightening) and ensure that proper safeguards and contingency plans are developed, implemented, and adequately tested.

The threats, their corresponding attacked system vulnerabilities, and resultant operational impacts provide the foundation to understanding risks. These understandings are integral to conducting the INFOSEC analyses as described in Section 4 (Phase 2 - Certification) as well as security, assurance, certification, and accreditation trade-offs. As described there, threats and risks will need to be re-analyzed throughout the development, operation, and maintenance of the system.

3.1.3.1 Threat Analysis

Historically, the threat analysis has not placed adequate emphasis on computer security (COMPUSEC) or networked systems. Identifying the threat of malicious logic attacks (e.g., viruses, worms, and computer misuse) is important to the security of the system. The threat analysis can also be used as input to the system threats and vulnerabilities, and risk analysis.

Potential threats can be organized into two basic hierarchial levels, namely, threat consequences and threat actions. Threat consequences define a negative effect that a threat may have on the secure operation of an information system. In contrast, threat actions define the potential causes for these consequences. Threat consequences include [4]:

✍ Disclosure: Any circumstance or event that may result in an individual or entity gaining access to information they are not authorized to receive. Exposure, interception, inference, and intrusion are threat actions.

✍ Deception: Any circumstance or event that may result in an authorized individual or entity receiving false information that is believed to be true. Masquerade, falsification, and repudiation are threat actions.

✍ Disruption: Any circumstance or event that interrupts or prevents the correct operation of the system services or functions. Incapacitation, corruption, and obstruction are threat actions.

✍ Usurpation: Any circumstance or event that results in the control of system services or functions by an unauthorized individual or entity. Appropriation and misuse are threat actions.

3.1.3.2 Preliminary Risk Analysis

Risk analysis is the process of analyzing threats to and vulnerabilities of an information system to determine the risks (potential for losses), and using the analysis as a basis for identifying appropriate and cost-effective countermeasures [1]. Countermeasures include technical, physical, personnel, and administrative. Risk analysis processes are used at each stage in the system life-cycle to aid in deciding whether the implementation of additional safeguards would be cost-effective with respect to reducing security risks [3] and should include the following:

- Identify system assets
- Identify and analyze threats to the system
- Identify and analyze vulnerabilities to the system
- Identify and analyze risks caused by threats acting upon vulnerabilities
- Identify countermeasures to mitigate risks

For additional information on risk analysis, refer to [12]. Risk analysis should be applied throughout the system life-cycle at key milestones/decision points (e.g., during requirements definition, completion of architecture, system installation) and is done to assist the CA in making decisions concerning the level of residual risk. lt should focus on (1) what can happen, (2) what are the consequences if the risk occurs, and (3) what is the possibility of the risk occurring. In determining the possibility of a risk occurring, the certification team should use the following criteria:

- The adversary is well equipped.
- The adversary uses sophisticated techniques.
- That such a well equipped, sophisticated adversary exists.
- The adversary is interested in performing the specified action.
- The adversary is willing to use the necessary capabilities.

3.1.3.3 System Capabilities

The functionality of the system will impact the level of effort required to certify the system. If the user has capabilities to store data locally or has access to system utilities (e.g., compilers, debuggers), the certification team must analyze the vulnerabilities and countermeasures associated with these capabilities. Using the previously determined minimum user clearance level and the highest data classification level, the mode of operation can be determined. Additional guidance on determining the mode of operation can be found in [5]. The mode of operation and the operating environment will greatly impact the amount and types of physical, personnel, and administrative security required.

3.1.4 Determine Certification Type

Before the C&A plan can be developed, the level of effort required to certify and accredit the system must be determined since there is tremendous variation in what the system may entail. The system being certified and accredited could range from a simple stand-alone personal computer (PC) to a large data center running dozens of applications on varied hardware platforms. It could range from a simple LAN connecting workstations for providing administrative support to a complex, distributed multilevel secure system. While the C&A process remains the same for any of these systems, the analysis to determine the appropriate level of effort, where to focus the analysis and testing, skills needed to perform the analysis, and supporting documentation may vary substantially. The analysis of security, from an INFOSEC perspective, needs to be simplified to ensure the appropriate level of resources are applied to the system C&A effort. The determination of certification type described in this section is based on the assumption that the certification (1) includes security controls from all INFOSEC disciplines and the interactions among these controls and (2) addresses threats against the stated objectives of availability, integrity, accountability, and confidentiality. Therefore, to assist system planners, particularly the CA, the concept of certification type is introduced.

3.1.4.1 Assurance Factors

A recertification type is the identification of the key aspects of any given system that have been determined to have a substantial impact on determining the appropriate level of effort. The certification type also includes detailed tasks to be performed as part of a system certification (i.e., tailoring the certification process). The degrees of assurance required for confidentiality, availability, integrity, and accountability are the factors used in determining the certification type. The user with minimal input from the Accreditor, PM and CA will determine which factor(s), if any, will be the driving component for determining the required degrees of assurance for the various categories. The main focus should be to recommend to the Accreditor the degrees of assurance required for the certification of the system and obtain approval from the Accreditor. Any major differences must be resolved before starting Phase II of the C&A process.

Assurance may be provided through four methods: (1) the way the system is designed and built; (2) analysis of the system description for conformance to requirements and for vulnerabilities; (3) testing the system itself to determine its operating characteristics; and (4) experience using the system. Assurance is also provided through documentation of the design, analysis, and testing [1].

The factors that guide degrees of assurance are described in Tables 3-1, 3-2, 3-3, and 3-4. These tables should be used as a guide in determining the degrees of assurance needed in the various categories, but are flexible to the system and environment. To use these tables correctly, refer to the consequences column on the left and identify the needed requirements of the system by selecting the appropriate weight (w=#). To facilitate reuse of certification evidence, the certification team should completely document its approach in determining the various degrees of assurance.

To assist the CA in completing Tables 3-1 through 3-4, the following terms are defined:

- Very likely: If the system fails to provide the specified service or the specified service fails, then at least 70% of the time the specified consequence will occur.

- Likely: If the system fails to provide the specified service or the specified service fails, then less than 70% of the time the specified consequence will occur.

- Operating budget: The annual budget of the organization that is responsible for the correct operation of the system (e.g., DoD funding for the Defense Message System (DMS) (not the entire DoD budget), Federal Government funding for the Internal Revenue Service (IRS) auditing system (not the entire IRS budget).

After completing Tables 3-1 through 3-4, the CA should total the weighing factors (w) and use Table 3-5 to determine the degrees of assurance for availability, confidentiality, accountability, and integrity. The amount of emphasis placed on each of these factors depends on the system criticality, the environmental requirements, and the system and functional requirements. To aid the CA in completing Tables 3-1 through 3-6, these tables are also included in Appendix E. The CA may reproduce the tables in Appendix E as needed and the completed tables should be provided as part of the certification package.

3.1.4.1.1 Confidentiality

Confidentiality services provide protection of information from unauthorized disclosure. Information may be disclosed in many ways, such as unauthorized user access, poor procedural controls, incorrect labeling of information, emissions, and interception. The following is a noncomprehensive list of the mechanisms that may be used to provide a confidentiality service [4]:

- Access control
- Object reuse
- Encryption
- TEMPEST techniques
- Separation of components
- Administrative procedures
- Physical security
- Fixed message length

Table 3-1 may be used to determine the degree of assurance required based on confidentiality requirements for the particular system.

Consequences of Loss of Confidentiality	**Confidentiality Weighing Factors**		
Impact of release of c from Appendix D, Table D-2)	data sensitivity >59 (w=8)	data sensitivity >=13 and <=59 (w=4)	data sensitivity <13 (w=2)
Loss of life from release of data	very likely (w=10)	not likely (w=5)	n/a (w=0)
Loss of credibility from release of data	very likely (w=5)	likely (w=3)	n/a (w=0)
Financial loss	>20% of operating budget per incident (w=5)	>*=50%* and <=20% of operating budget per incident (w=3)	<5% of operating budget per incident (w=l) n/a (w=0)
Civil penalties/fines	>=$10,000 per incident (w=5)	<$10,000 per incident (w=3)	n/a (w=0)

TABLE 3-1 Confidentiality Metric

3.1.4.1.2 Integrity

Integrity services provide protection from information or resources being created, inserted, modified, or deleted by entities not authorized for these actions. Integrity protection may include the prevention or detection from these actions, and may also provide capabilities to recover from successful attacks on the integrity of a system [4]. Additionally, it may be necessary to prevent users from inadvertently impacting the integrity of the data or the system.

The following is a noncomprehensive list of mechanisms that may be employed to provide integrity services:

- Access control
- Checklist
- Digital signatures
- Recovery mechanisms
- Nonvolatile memory
- Deterrence
- Configuration control
- Secure maintenance of components
- Inspection of hardware/firmware/software (to include diagnostic routines)
- Comparison with known correct components
- Administrative procedures
- Physical security

Table 3-2 may be used to determine the degree of assurance required based on integrity requirements for the particular system [11].

Consequences of Loss of Integrity	**Integrity Weighing Factors**		
Loss of credibility from integrity failure (system or data)	very likely (w=5)	likely (w=3)	n/a (W=0)
Loss of life from integrity failure (system or data)	very likely (w=10)	likely (w=5)	n/a (w=0)
Civil penalties/fines for integrity failure	>=$10,000 per incident (w=5)	<$10,000 per incident (w=3)	n/a (w=0)
Financial loss from integrity failure	>20% of operating budget per incident (w=5)	>*=50%* and <=20% of operating budget per incident (w=3)	<5% of operating budget per incident (w=l) n/a (w=0)

TABLE 3-2 Integrity Metric

3.1.4.1.3 Availability

Availability services provide protection to make system capabilities accessible and/or operational to ensure that information can be obtained by authorized entities. Availability protections allow the system and/or individual components of the system to meet user-specified requirements for unobstructed operations and allow the system to make information accessible to the users when needed. The following is a noncomprehensive list of mechanisms that may be used to provide availability services [4]:

- Access control
- Hardware redundancy
- Information backup
- Anti-tamper mechanisms
- Anti-jam mechanisms (e.g., frequency hopping)
- Facilities hardening
- Modularity
- Operations security

Table 3-3 may be used to determine the degree of assurance required based on availability requirements for the particular system [11].

Consequences of Loss of Availability	**Availability Weighing Factors**		
Loss of credibility from system failure	very likely (w=5)	likely (w=3)	n/a (W=0)
Loss of life from system failure	very likely (w=10)	likely (w=5)	n/a (w=0)
Financial loss from system failure	>20% of operating budget per incident (w=5)	>*=50%* and <=20% of operating budget per incident (w=3)	<5% of operating budget per incident (w=l) n/a (w=0)
Disruption of critical service[1]	very likely (w=4)	likely (w=3)	n/a (w=0)
Civil penalties/fines for loss of availability	>=$10,000 per incident	<$10,000 per incident	n/a (w=0)

	(w=5)	(w=3)	

TABLE 3-3 Availability Metric

3.1.4.1.4 Accountability

Accountability services provide the capability to verify the identity of various entities that initiate system events and allow reliable auditing of these events. Accountability includes authenticity and non-repudiation. Accountability validates and documents that an entity attempted to initiate a process or system even that an event or process was initiated, who sent a message, that a message was sent, who received a message, and that the message was received. The following is a non-comprehensive list of mechanisms that may be used to provide accountability services:

- Identification and Authentication
- Physical access controls
- Trusted Computing Base (TCB)
- Anti-spoof
- Passwords and digital signatures
- Cryptography
- Event auditing

Table 3-4 may be used to determine the degree of assurance required based on accountability requirements for the particular system.

Consequences of Loss of Accountability	**Accountability Weighing Factors**		
Civil penalties/fines for loss of accountability	>=$10,000 per incident (w=5)	<$10,000 per incident (w=3)	n/a (w=0)
Loss of life from accountability failure	very likely (w=10)	likely (w=5)	n/a (w=0)
Loss of credibility from accountability failure	very likely (w=5)	likely (w=3)	n/a (w=0)
Financial loss from accountability failure	>20% of operating budget per incident	>=50% and <=20% of operating budget per incident	<5% of operating budget per incident (w=l)

	(w=5)	(w=3)	n/a (w=0)

TABLE 3-4 Accountability Metric

3.1.4.2 Assurance Ranges

The assurance ranges are the result of analyzing the results from Tables 3-1, 3-2, 3-3, and 3-4. After completing Tables 3-1, 3-2, 3-3, and 3-4 and summing the weights (w=#) for each assurance category, the CA may use Table 3-5 to determine the degrees of assurance for each category. When using Table 3-5, the CA, with the assistance of the User Representative, PM, and Accreditor, may choose to raise any of the degrees of assurance required. For example, if the weight factor for availability is 16 (medium), but if the system fails there could be severe risk of loss of life, the CA may choose to raise the degree of assurance for availability to high. This fact should be clearly documented by the CA. On the other hand, care must be taken if the CA lowers any of the degrees of assurance, and the reasons for this must be clearly documented and approved by the Accreditor. These degrees of assurance are also used in Chapter 4 to assist the CA in determining the level of effort for the specified tasks.

Assurance Categories	Assurance Ranges		
	High	Medium	Low
Confidentiality (from Table 3-1)	w > 18	w >= 6 and <= 18	w < 6
Integrity	w > 14	w >= 4 and <= 14	w < 4
Availability (from Table 3-3)	w > 17	w >= 5 and <= 17	w < 5
Accountability (from Table 3-4)	w > 14	w >= 4 and <=14	w < 4

TABLE 3-5 Assurance Ranges

3.1.4.3 Degrees of Assurance

During this activity, Table 3-6 is used to determine the type of certification to perform. Using the degrees of assurance and the type of certification, tailoring of the system analysis can begin. As an example, for COMPUSEC, lower degrees of assurance do not require formal models to verify that the security policy is enforced by trusted security mechanisms (e.g., TCB). Systems that require higher degrees of assurance may require, through the use of formal models and additional documentation and testing, that the trusted security mechanisms enforce the security policy. This example only considers data confidentiality. As another example, for TEMPEST, depending on the threat and degrees of assurance needed, different rules can be applied for identifying control zones for systems that may have compromising emanations. Also, depending on the sensitivity, environment, and degrees of assurance, a variety of tamper proof techniques can be implemented in COMSEC products and/or modules.

Assurance Ranges	Certification Type
If the total of the weighing factors (Tables 3-1 through 3-4) for confidentiality, integrity, availability, and accountability are < 16	Type 1
If the total of the weighing factors (Tables 3-1 through 3-4) for confidentiality, integrity, availability, and accountability are >=16 and <= 30	Type 2
If the total of the weighing factors (Tables 3-1 through 3-4) for confidently, integrity, availability, and accountability are > 30 and <= 62	Type 3
If the total of the weighing factors (Tables 3-1 through 3-4) for confidentiality, integrity, availability, and accountability are > 62	Type 4

TABLE 3-6 Certification Type

When the tailoring factors have been applied to the certification effort, the CA should begin selecting members for the certification team. The first task of the certification team should be to develop the C&A plan jointly with the PM using the certification type. The C&A plan should clearly specify how the tailoring factors should be used in determining the depth and breadth of the system analysis and testing. For example, if the degree of assurance for integrity is high, but all the degrees of assurance for availability, confidentiality, and accountability are in the low range, the certification team should focus its efforts on the tasks identified in Chapter 4 that analyze the integrity of the system. The certification team must understand that the numbers derived from using Tables 3-1 through 3-5 only provide a rough order of magnitude (ROM) (e.g., high, medium, low) for the degrees of assurance and should be used accordingly.

3.1.4.4 Types of Certification

Now that the assurance ranges that will influence the level of effort for the certification have been established, the certification team can determine the type of certification for the system. The CA will make the decision, based on Tables 3-1 through 3-6 as to the type of certification to be performed. The type of certification should be approved by the Accreditor prior to the start of the tasks described in Chapter 4. Unfortunately, if the assurances ranges are widely skewed (e.g., confidentiality and integrity low, accountability medium, and availability high), this will affect the type of certification to be performed and the amount of analysis to be performed. If this situation occurs, the certification team should use the degrees of assurance as an aid in determining the tasks to be completed and the level of effort to be expended on each of the tasks.

3.1.4.4.1 Checklist 👓 Type 1

The checklist certification (Type 1) is the simplest type of certification to conduct. This type of certification involves completion of the checklist in Appendix F which includes verification that procedures for proper operation are established, documented, approved, and followed.

3.1.4.4.2 Abbreviated Certification 👓 Type 2

The abbreviated certification (Type 2) is more extensive than the Type 1 certification, but should also include completing the Type I checklist. The amount of documentation required and the resources devoted should be minimal. The focus on this type of certification is INFOSEC functionality (e.g., auditing, access control, I&A). Minimal evidence is required for this type of certification.

3.1.4.4.3 Moderate Certification 👓 Type 3

The moderate certification (Type 3) is more detailed and complex, and requires more resources. This type of certification is generally used for systems that require the highest degrees of assurance, have a greater level of risk, and/or are more complex. The focus on this type of certification is also on INFOSEC functionality (e.g., auditing, access control, I&A); however, more extensive evidence is required to show that the system meets the security requirements.

3.1.4.4.4 Extensive Certification 👓 Type 4

The extensive certification (Type 4) is the most detailed and complex type of certification and generally requires a great deal of resources. This type of certification is used for systems that require the highest degrees of assurance and may have a high level of threats and/or vulnerabilities. The focus on this type of certification is INFOSEC functionality (e.g., auditing, access control, identification and authentication) and assurance. Extensive evidence, generally found in the system design documentation, is required for this type of recertification.

3.1.5 Identify C&A Team

The CA may obtain assistance from many other organizations to analyze the system throughout its life-cycle. The CA is the individual(s) responsible for making a technical judgment of the system's compliance with the stated security requirements and to identify and analyze risks. In addition, the CA has the responsibility for coordinating the various activities of the certification effort, merging the results of those activities, and preparing the certification package [18]. The CA should take this into consideration in planing the required training and team composition. Once the CA knows the type of certification and the tasks to be performed (discussed in Chapter 4), the composition of the certification team can begin. From the tasks identified, the expertise required by the individual team members can be determined.

3.1.5.1 Determine Composition of Certification Team

The composition of the team should depend on the size and complexity of the system under examination. There should be someone with risk management risk analysis, or operations experience. Individuals with these disciplines should have the background to perform the risk analysis and security countermeasures trade-off examination [18].

The certification team, which reports to the CA, is a collection of individuals and organizations involved with the certification process. For some systems (e.g., a large acquisition, a complex distributed system), a certification team may be necessary to direct certification activities and identify/resolve security-related issues throughout the system development life-cycle and operation of the system. Once a team is formed, it should become knowledgeable of the entire C&A process described in this handbook, not just the task(s) and activities each team member is responsible for. The team may include the Accreditor's representative, whose role is to identify, address, and coordinate security accreditation issues with the Accreditor [18].

Certification should be performed by competent technical personnel independent of the system developer. Given the increasing complexity of many systems and the wide variety of security disciplines that must be analyzed during certification, one organization may not have adequate or appropriate in-house resources to perform many of the required certification activities (e.g., detailed evaluations, testing). To perform some of these activities, the CA may rely on the resources of other organizations or contractors that have the necessary specialized skills [18].

Since some of the security requirements of a system can be addressed by non-technical means, a close relationship should be established with the organization providing physical security. These individuals may assist in site surveys, administrative security analysis, and countermeasures analysis. Although the funding and training organizations are not directly involved in the security and certification of the system, their support will be needed in planning for the certification effort. Appendix C (Table C-1) identifies the individuals who may assist in the certification, but may not be considered part of the certification team. The CA should consider the following items when selecting members for the certification team:

- Whether the individual is needed full-time/part-time
- The clearance requirements
- Prior C&A experience requirements
- Prior testing experience requirements
- Required INFOSEC knowledge (e.g., trusted products, COMSEC, COMUSEC, TCB evaluations, physical security, administrative security)
- Length of time required on the certification team
- Training (system and C&A) requirements

3.1.5.1.1 Determine Team Organization

The certification team may be a matrix of individuals from various agencies who are temporarily detailed to assist with the certification. This type of organization will allow the CA to obtain specialists in the required INFOSEC disciplines who may not be available in-house. The CA must be aware that these individuals may not be available full-time to work on the certification and should schedule their time accordingly. Also, they may have limited experiences in performing a certification.

In large system development organizations, a C&A office may exist. This office should be staffed with personnel who have the required INFOSEC and C&A expertise. The major obstacle the CA must overcome is the availability of these individuals to perform the certification. The priority of the system, its degrees of assurance, and the budget of the C&A official will have a major impact on the scheduling of the various C&A tasks.

3.1.5.1.2 Identify Team Duties and Responsibilities

The certification team normally manages and performs security-related activities that include identifying and interpreting security regulations and standards, preparing, and/or reviewing, INFOSEC portions of the Request for Proposal (RFP), reviewing major acquisition strategy decisions for certification considerations, and managing certification issues. Ideally, the technical security representatives from, or consultants to, the appropriate participating organizations should be involved in these activities [18]. All team members should be knowledgeable of at least the following items:

- Role of the Accreditor
- Requirements of the Accreditor
- C&A schedule
- Level of effort
- Interactions with other groups
- Individual responsibilities

3.1.5.1.3 Conduct Team Training

A major obstacle to successfully completing a certification is scheduling and receiving sufficient system-specific training (e.g., application software, operating system) at an appropriate time. This is particularly true for the matrix organization since certification is not its primary responsibility. If this type of organization is used, the individuals should be identified early enough so they can schedule and obtain the necessary training. The CA may also provide support to the testing organization in return for training, funds and courses. Most testing organizations are understaffed and are always looking for additional support. This should include system-specific (e.g., operations, system design, tools) and C& specific (e.g., architecture analysis, TCB identification, communications protocols, networks) training.

3.1.5.2 Interact with Other Groups for C&A Support

The CA must establish an early relationship with the Accreditor, in order to understand the concerns and requirements of the Accreditor, and with the various working groups involved with the system. Most of the groups discussed in the following paragraphs may exist in some form, and the CA should develop a close working relationship with these groups. One area that should be addressed early in the process is the level of residual risk the Accreditor is willing to accept and the level of effort the Accreditor expects from the certification team. For larger systems, the Accreditor may establish an accreditation team. If this is the case, the CA should work very closely with the accreditation team leader. An accreditation team is a management tool that represents the Accreditors' concerns throughout the development process.

3.1.5.2.1 Accreditation Team

For a small or simple system, an accreditation team may not be necessary. These functions could be performed by either the Accreditor (or their representative) or by the CA. However, a complex system or large network may require a team to analyze the data gathered and presented by the certification team. When there are multiple Accreditors, an accreditation team is recommended to resolve accreditation issues that may arise and to formulate the MOA among the Accreditors [18].

3.1.5.2.2 Configuration Management

A configuration control system should be established early in the system development (probably as soon as the requirements are established and agreed to) and continue until the system is removed or replaced. Although the certification team is not responsible for implementing a configuration control system, the certification team must understand the configuration control process in order to determine its strengths and weaknesses. The analysis of the configuration management system is discussed in Chapter 4. At this point, the certification team should identify the developer(s)/maintainer(s) of the software, hardware, and firmware. If applicable, both the Government PM and the contractor PM must be identified. In most configuration control systems, various boards are established and their responsibilities identified. The certification team must identify the individual who is responsible for allowing changes to the system. This authority usually resides with the chairman of the Configuration Control Board (CCB).

If the system requires a high degree of assurance in integrity and availability, the certification team should work closely with the vendor or the logistical support organization to obtain data on mean-time-between failure to analyze the reliability, maintainability, and availability (RMA) of the system's components. This analysis is fairly straightforward for hardware; however, RMA data on software, at the module level, is usually not available.

3.1.5.2.3 Information Systems Security Working Group (ISSWG)

The Accreditor, User Representative and PM may elect to form an ISSWG. This informational working group serves as the forum for all parties involved with the system, to review and resolve the security issues, and monitor the C&A activities. The CA should be a member of the ISSWG when formed. The composition of the group will vary depending on the system life-cycle phase and organizations involved, and may include the integrator, possible key product vendor representatives, application developers, etc.

Responsibilities of the ISSWG are to assist the PM Accreditor and User Representative in the resolution of security issues and ensure the users' needs are met. Appendix C (Table C-2) contains a list of the recommended representation in the group, including responsibilities. These responsibilities are not to be confused with the responsibilities of the three principals the DAA, PM and User Representative.

3.1.5.2.4 Test Coordination

The CA should also be involved with the Test Planning Working Group since some of the assurance is provided through testing. This group is responsible for planning, coordinating, scheduling, and performing the various tests on the system. Since a major portion of the certification effort involves testing the system, the certification team should be represented in this group and this group should assist the certification team in the development of the certification test plan used in Chapter 4, Activity 3. Many of the tests performed by this group may be used as documentation for the certification test plan and duplicate tests may not be required. The security-relevant tests may be included in the various other tests to use the limited system testing time more effectively. At a minimum, the certification team should review all test plans and procedures and receive a copy of all security-relevant test reports.

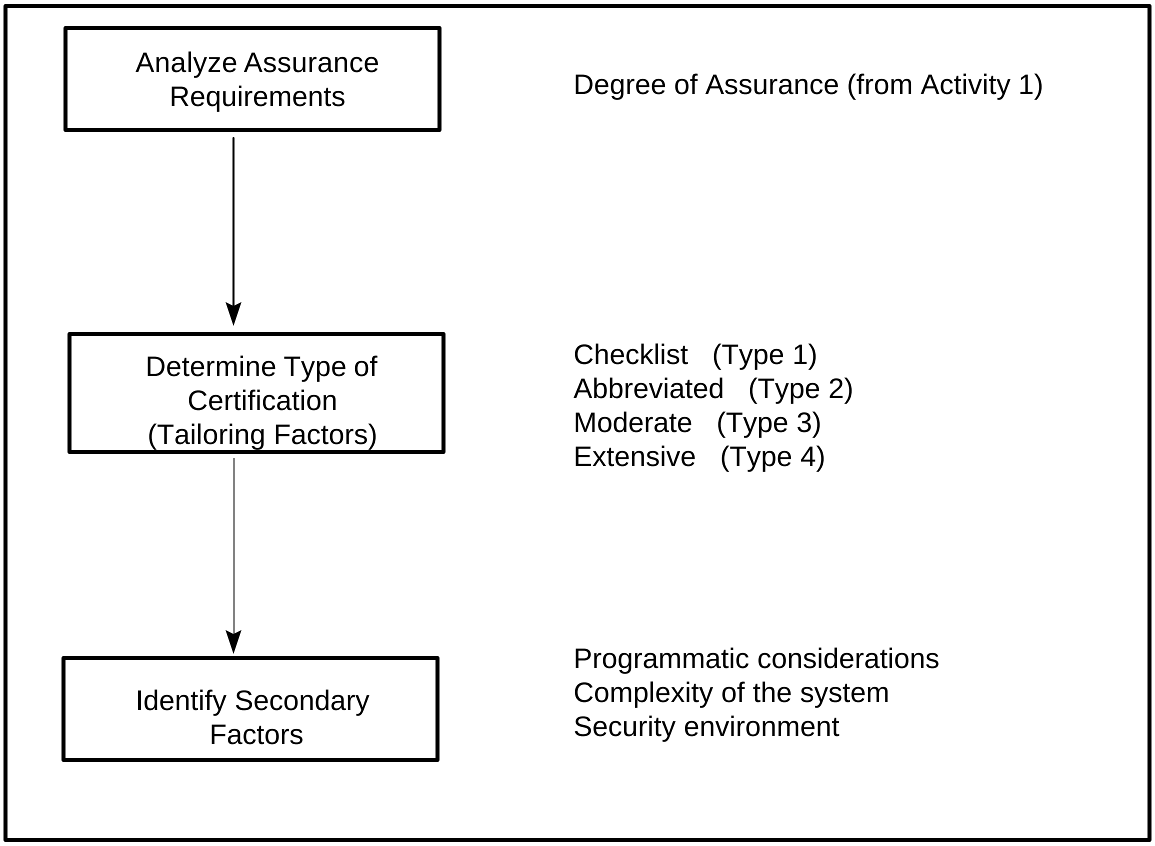
3.1.6 Prepare Certification Agreement

Using the information gathered in the preceding tasks, the CA should document the information in a Certification Agreement, Appendix G. When this is completed, the agreement should be submitted to the DAA, PM and User Representative for approval. The Certification Agreement is designed to meet the requirements of OMB A-130, Appendix III. It establishes the amount of effort or what needs to be done and thus forms the basis for the C&A Plan.

3.2 Activity 2 - Plan for C&A

The second activity is to develop the C&A plan. The twofold purpose of this activity is to plan the C&A effort and to identify and obtain all necessary resources. C&A planning activities are based on information collected during Activity l. The plan should (1) identify programmatic considerations, (2) determine applicability of available certification or evaluation evidence, (3) determine the composition of the certification team, (4) identify technical skills or resources, (5) incorporate C&A milestones into program/project milestones, and (6) document C&A planning information.

Although planning for C&A is a separate activity in the process, plans must be flexible enough to sustain minor changes or delays in the system development. During each activity in the C&A process, the plan must be reviewed and any necessary modifications made. The C&A plan should be integrated into the system development plan. The basic strategy is to develop a comprehensive plan, obtain agreement from all the players (most importantly, the Accreditor), and then execute the plan. When completed, the C&A plan should be submitted to the PM, Accreditor, and User Representative for review and approval [13].


Analyze Assurance Requirements
Degree of Assurance (from Activity 1)
Determine Type of Certification (Tailoring Factors)
Checklist (Type 1)
Abbreviated (Type 2)
Moderate (Type 3)
Extensive (Type 4)
Identify Secondary Factors
Programmatic considerations
Complexity of the system
Security environment

3.2.1 Identify Secondary Factors

Another major consideration in determining the level of effort for the certification and developing the certification plan involves the life-cycle status, complexity of the system, and the security of the development/maintenance environment. For example, if the system is still under development, the Accreditor, with technical assistance from the security engineer/ architect, should be able to direct the development of the system from the aspect of security. At the conclusion of this activity, the CA must provide the Accreditor with a basic strategy on how the system will be certified, and the Accreditor must approve the approach. Refer to Figure 3-2.

Figure 3-2 Certification Tailoring Tasks

3.2.1.1 Identify Programmatic Considerations

The C&A plan integrates the C&A activities with the system development or modification. It is stressed that the CA must integrate the C&A activities with the developing and/or maintaining organizations and their plans for their systems. To accomplish this, the CA must work closely with the PM and system maintainers to tailor the C&A plan to the acquisition strategy of the PM. The C&A

plan should be agreed to by the CA, Accreditor, PM and the User Representative.

3.2.1.1.1 New System Acquisition

During new system acquisition, the Accreditor and the certification team should become involved during the system's requirements generation. This early involvement should address items such as development of the security policy, identification of security testing requirements, determination of the degrees of assurance, and identification of the C&A activities. The effectiveness of the certification process is greatly enhanced by making it part of the systems endearing development process. The intent is not to produce and manage a separate process, but to tie the activities required for C&A to the established engineering and life-cycle milestones. Certification timing and phasing thus become integral to the system development cycle. The objectives are to (1) to schedule, gather and report certification information throughout system development, (2) establish reasonable checks and balances within the process, (3) avoid unexpected issues and problems just prior to Initial Operational Capability (IOC), and (4) make accreditation and the subsequent reaccreditation a more straightforward process. The ground work and data gathering, as well as concurrence from all parties involved, have already been completed [14].

3.2.1.1.2 Incremental Build

For this type of acquisition strategy, the PM, Accreditor, and CA should determine the security impacts for each increment and include in the C&A plan the increments that will need to be certified and accredited. The initial and final increments should always be certified and accredited. The Accreditor may accredit each increment specifying that the previous certification is still valid or the Accreditor may specify in the C&A plan that only certain increments need to be certified and accredited. The point to remember is to determine when and if each increment will need to be certified and/or accredited and plan the necessary resources accordingly. The certification agreement should be used as the basis to determine which increments need to be certified and accredited and the CA must ensure that the certification agreement is updated.

3.2.1.1.3 Follow-On or Upgrade to Existing System

For existing systems going through an upgrade, the C&A effort may be dependent on the quality of the previous certification, if any exists. The Accreditor must become involved early in the decision to upgrade the system to ensure that (1) security is provided in or between the upgraded components, (2) security weaknesses in the existing/non-upgraded components are analyzed and appropriate countermeasures implemented, (3) inadequate components (from a security perspective) are replaced as part of the upgrade, and (4) transition to the upgraded system is securely accomplished. Appendix H contains a non-inclusive list of changes that would constitute an upgrade to an existing system.

Most likely, the request for the modification will be driven by (1) a new user requirement, (2) a new threat identified, or (3) a change in a technology (e.g., commercial-off-the-shelf (COTS) hardware or software products). No matter what the driving factor for the modification, the request should be processed through a Configuration Management (CM) system. As part of the CM process, the request should be reviewed and approved or disapproved by the CCB. The CCB should determine whether this change requires a reaccreditation and possible recertification of the system. The Accreditor should be involved in making this determination.

3.2.1.1.4 Existing System

When faced with performing a certification of an existing operational system, the certification team should take into consideration several factors. First, the projected life of the system should be determined. If the system will be replaced within several years, the Accreditor may accept a higher degree of residual risk until a new system is operational. Also, the certification team should determine if any major modifications are projected for this system and include this modification in the baseline for the certification. Because this is an operational system, some of the required security documentation may be obtained by reviewing any previous operational problems and updates to the system. Lastly, the availability, adequacy, and correctness of the documentation may not provide enough information to satisfactorily complete some of the tasks listed in Chapter 4.

3.2.1.1.5 Prototype or COTS Integration

The certification team should be wary of systems that are considered prototype or COTS integration. The system is a new acquisition and may not follow a full-scale development model. For a prototype system, the certification team must consider the possibility that the system will be installed and used operationally. If this is the case, the certification team should consider the system a new acquisition and follow the procedures for a new acquisition as appropriate.

With COTS integration, the certification team should consider the amount of software that must be developed to integrate the various COTS components and the security ramifications of using each of the COTS components. If a vast amount of security-critical software must be developed, more analysis and testing may be required. However, COTS integration security requires the C&A process be followed.

3.2.1.2 Determine System Complexity

The complexity of the system is dependent on the complexity of the hardware, software, interfaces to other AIS environments, and how the various users gain access (e.g., workstation, dumb terminal) to the system. The complexity of the hardware is dependent on the effort required by the vendor to integrate the various components into the final system architecture. The complexity of the software is dependent on the amount of unique software that must be developed to integrate the various COTS/Government-off-the-shelf (GOTS) hardware and software components of the final system and how well the unique software and hardware are documented and their functions understood. User complexity is dependent on how many users have simultaneous access to the system, how these users gain access to the system, and the amount of functionality (e.g., menus and privileges) given to various groups of users. The less control the system administrator has over the various users, the greater the level of user complexity. The system complexity should drive the level of effort required to analyze the system security architecture discussed in Chapter 4.

3.2.1.3 Identify Security Environment

With the increased use of COTS products, the environment in which the COTS product is developed and maintained becomes a critical factor to the degrees of assurance, especially in regard to malicious code. [16] makes a distinction between an open and a closed security environment. If the software, COTS or developed, or hardware is developed and maintained by trusted individuals and controls are implemented to protect against introduction of malicious logic, then the level of effort for reviewing the security-critical portion (e.g., TCB) may be reduced.

3.2.2 Determine Applicability of Documentation

During the plan for C&A Activity, the certification team should determine the applicability of any available documentation and the need for any additional documentation. The requirement for system and security-related documentation should be driven by the suggested documentation for the required tasks and contents of the certification package, both discussed in Chapter 4. Appendix I contains a detailed description of the contents of the certification package. If some documentation is unavailable or infeasible to create, the Accreditor should be made aware of this fact and the risks associated with not having the suggested documentation.

Some of this documentation may be obtained from product evaluation reports, product profiles, evidence from similar certifications, or previous component (e.g., facility) assessments. In addition, the certification team should identify all baseline documentation that addresses security issues and controls. If no evaluation reports (e.g., product evaluation reports, product profiles) exist for a product enforcing a security requirement, the CA must plan the time and resources needed to develop the required documentation. Suggested documentation includes [17]:

- Functional requirements
  - Design specifications
  - Maintenance manual
  - Operator's manual
  - User's manual
  - Information flow charts
  - Algorithms
  - Sample input/output documents
  - Management policies and procedures
  - Diagrams of network connections
  - Operating procedures
  - Trusted Facility Manual (TFM)
  - Security Features User's Guide (SFUG)
  - Security models

3.2.3 Develop C&A Plan

Scheduling of the required tasks described in Chapter 4 must be addressed to ensure availability of personnel, facilities, and necessary resources. Careful planning will reduce scheduling conflicts and delays in accomplishing testing [13]. The planning emphasis should be directed to areas having a greater potential for loss of, or risk to, sensitive information. These areas may have been identified in an earlier risk analysis, problems identified during testing, or in reports of past problems with similar systems [13].

3.2.4 Obtain Approval of the C&A Plan

The Certification Agreement and the C&A Plan form the basis for the ensuing C&A effort. The certification agreement and C&A Plan document the security requirements, tailoring, intended operating environment, risk-related considerations, level-of-effort, and the C&A schedule. As such, the agreement and plan are submitted to the PM, DAA, and User Representative for approval before the effort continues.

SECTION 4

PHASE II: CERTIFICATION

Phase II includes two Activities: (1) perform an analysis of the system, and (2) report findings/recommendations. The analysis is dependent on the tailoring factors identified in Activity 1. This phase also helps the certification team analyze the potential vulnerabilities and associated operational risks by revisiting the threat and risk analyses conducted in the Pre-Certification Phase. These analyses will be used during the architectural, design, and implementation work. In fact, threat, vulnerability, and risk analyses will be conducted several times as this work progresses. The final threat and risk analysis will assist the Accreditor with the accreditation decision. The areas of risk on which the certification team should focus are the protection of information from unauthorized access by individuals, denial of service with regard to deliberate attempts to disrupt the access to and processing of information, assurance that the integrity of information and system is maintained, and assurance of accountability. During this phase, the certification team should routinely visit the operational site to analyze the system capabilities from an INFOSEC perspective.

System security measures are typically based on system security policy and operational requirements. It must be emphasized that to provide a realistic and effective evaluation of the security posture of a system, all appropriate security disciplines (an integrated INFOSEC perspective) must be included in the certification. The security disciplines include:

- COMPUSEC
- COMSEC (e.g., transmission security (TRANSEC), crypto security)
- Physical security
- Operations security (OPSEC)
- TEMPEST
- Personnel security
- Industrial security
- Other security disciplines should also be considered (e.g., electronic security)

4.1 Activity 3 - Perform INFOSEC Analysis

System analysis represents Activity 3 of the C&A process. These tasks verify by analysis, inspection, and testing that the information security requirements have been correctly implemented and function correctly. The level of analysis and testing must be approved by the Accreditor. In performing the system analysis, the following three major tasks must be performed:

- Analyze detailed system information
- Conduct INFOSEC analysis (e.g., documentation review, testing, architecture studies)
- Conduct a vulnerability assessment and risk analysis

Each of these tasks represent a critical aspect of system certification. Analyzing deed system information involves a detailed review of system documentation gathered in Activity 1 to determine if and how the system security requirements have been met and to determine where to focus the system analysis and testing. This activity is performed in preparation for system testing, to prepare documentation (e.g., certification test plan), and to verify if the security features are in place and meet the appropriate security requirements.

When conducting the INFOSEC analysis, each task must be conducted and the results viewed from an INFOSEC perspective to analyze trade-offs between solutions in the various INFOSEC disciplines. This activity builds upon the knowledge gained during the detailed system analysis. The level of testing and analysis for each discipline will vary depending upon the mission of the system and the assurance requirements.

Currently, 21 tasks have been identified for the four types of certification. If some of the specified tasks cannot be performed, this limitation should be reported as a risk and the Accreditor should determine if the risk of not performing the task is or is not acceptable. By using Table 4-1 and the type of certification listed in Table 3-6, the minimum tasks for each type of certification can be determined. Several of the tasks specified in Table 4-1 are applicable to more than one type of certification. In this case, the task description will specify the level of effort required for the applicable types of certification. Also, some of the tasks contain subtasks and each task may have one or more prerequisite tasks. The main driving factors for determining the level of effort are the system complexity, acquisition strategy, and security environment discussed in Chapter 3.

4.1.1 Analyze Detailed System Information

The first Activity in this Phase involves two major tasks: (1) development of the detailed analysis of the documentation and the system information that was collected during the Pre-Certification Phase (Activity 1), and (2) the preparation of additional certification documentation (e.g., test plans and procedures). The documentation to be reviewed must include information addressing the level of sensitivity and classification of the data and system interfaces. Additionally, procurement-related documents (e.g., SOW, system specification) and the suggested documentation should be reviewed. The certification team should be directly involved in the design reviews to assist the certification team members in completing some of the required tasks.

Certification Tasks	Type of Certification			
	Type 1	Type 2	Type 3	Type 4
System Security Architecture				
1. System Architecture Study	X	X	X	X
2. Identify TCB Boundary			X	X
3.Software, Hardware, Firmware Architecture Study			X	X
4. Interface Analysis		X	X	X
5. Covert Channel Analysis[1]		X	X	X
6. Composition Analysis		X	X	X
Life-Cycle Analysis				
7. CM Plan Review/Audit		X	X	X
8. Developmental Suite CM Review			X	X
Testing				
9. Coverage Analysis of Test Suite		X	X	X
10. Requirements Traceability		X	X	X
11. Security Functional Testing		X	X	X
12. Reliability Testing		X	X	X
13. Penetration Testing		X	X	X
14. TEMPEST Testing [2]		X	X	X
15. COMSEC Testing [3]		X	X	X
16. Contingency Plan Testing		X	X	X
Physical Security Testing				
17. Facility Perimeter Analysis		X	X	X
18. Environmental Control Analysis		X	X	X
Operational Security Review				
19. Minimal Security Checklist	X	X	X	X
20. Operational Procedure Review	X	X	X	X

21. Vulnerability Analysis		X	X	X

TABLE 4-1 INFOSEC Analysis Tasks

1. Only applicable if degree of assurance for confidentiality is high (Table 3-5)
2. Not applicable if there is no TEMPEST requirement
3. Not applicable if there is no COMSEC requirement

4.1.2 Conduct INFOSEC Analysis

This task in the System Analysis Activity involves understanding the actions, objectives, and steps to be performed for each INFOSEC discipline based on the degrees of assurance determined from Table 3-5. An analysis of each discipline is conducted, focusing on the degrees of assurance, but considering the secondary factors to ensure the appropriate level of resources are applied to each discipline. The analysis of each discipline is also based on the type of certification required (i.e., Type 1, 2, 3 or 4). After selecting the type of certification from Table 3-6, documents required and steps to be performed will vary. The analysis to be conducted will also vary.

An INFOSEC analysis is performed to determine if the system meets the requirements as specified in the security policy and reviewed in the Pre-Certification Phase. The certification team must be provided an appropriate level of design documentation and training on the system as both administrators and general users and should be able to design and implement test programs for the system.

Obtaining the appropriate level of design documentation is critical to performing the design analysis. If the component, or a product used in the system, has been evaluated by the National Security Agency (NSA), the Final Evaluation Report (FER) or product profiles will identify the security mechanisms the component provides, as well as detailed information on how those mechanisms work. The certification team should verify the applicability of each product to the system security requirements. If the certification team cannot obtain a FER or product profile (the component has not been evaluated or is currently being evaluated), the same level of design information must be obtain from the developer and made available to the analysts. The certification team should have a liaison with the system developer (e.g., contractor, vendor) to obtain the necessary documentation and resolve any questions.

There are several inputs that can be used to conduct the INFOSEC analysis. These inputs include:

- C&A Plan
- Certification agreement
- Evidence from similar certifications
- Previous component assessments
- Analysis and constraints on interconnected systems
- System design descriptions

- System source code

The tasks performed during the INFOSEC analysis, as well as the time spent on analysis, are commensurate with the required degrees of assurance. The objectives of the following tasks are to ensure the system provides an appropriate level of protection and to identify any deficiencies in the protection mechanisms. At the completion of each task, a summary report should be completed detailing the steps performed, the time and resources used, problems and limitations encountered, and strengths and/or weaknesses found. These summary reports should be included in the certification package and will greatly reduce the time required to recertify the system or aid in the recertification of similar system. A sample report format is provided in Appendix J.

4.1.2.1 System Security Architecture

The system security architecture is the physical representation of the security policy, the CONOPS, and the functional requirements. It focuses on those aspects of the overall architecture that identify security services and mechanisms, allocates security-related functionality to system components or configuration items (CIs), and identifies interdependencies among the security-related components [4]. System security architecture consists of system architecture, software architecture, interface analysis, covert channel analysis, TCB identification, and composition analysis. The intent of the system security architecture analysis is to identify how effectively the system architecture enforces the security policy and implements the security requirements. The interfaces must be evaluated to assess their effectiveness in maintaining the security posture of the infrastructure.

Task 1: System Architecture Study

Task Objective: Ensure the system architects supports and enforces the security policy.

Task Description: The architecture study involves, but is not limited to, analyses of the following:

- How the system was designed
- Where the security-relevant components are located
- Overall architecture of the system
- Allocation of the security features
- Identification of the critical interfaces
- Identification of connections to external networks and systems
- Type of equipment used to develop the target system

Prerequisite Tasks: None

Suggested Documentation: Security Policy, System Architecture, System Design Specifications, Descriptive Top-Level Specification (DTLS), System design review documentation, additional for Type 4; Formal Top-Level Specification (FTLS)

Suggested References: *Trusted Database Management System Interpretation* (NCSC-TG-021), *Assessing Controlled Access Protection* (NCSC-TG-028), *A Guide to Understanding Design Documentation in Trusted Systems* (NCSC-TG-007), *A Guide to Understanding Trusted Recovery in Trusted Systems* (NCSC-TG-022), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority Scheme for EDP Audit and Computer Security Review* (NBSIR 86-3386)

Type 1 Level of Effort: If the system is connected to other systems or networks, evaluate the network interfaces using the minimal security requirements checklist.

Type 2 Level of Effort: Ensure the components of the entire system have been identified. Determine the purpose and functionality of each component in regard to supporting the security policy.

Type 3 Level of Effort: Ensure the components of the entire system have been identified. Determine the purpose and functionality of each component in regard to supporting the security policy. Ensure the interfaces of the components have been identified. Determine the adequacy of the development equipment suite to support the target architecture.

Type 4 Level of Effort: Ensure the components of the entire system have been identified. Determine the purpose and functionality of each component in regard to supporting the security policy. Ensure the interfaces of the components have been identified. Determine the adequacy of the development equipment suite to support the target architecture. Identify all subjects and objects, and ensure that the references monitor concept (e.g., enforcement for authorized ass relationships between subjects and objects) has been implemented correctly.

SubTask 1a: Network Connection Analysis

Task Objective: Analyze the connections to other systems and/or networks to ensure that network and overall system security polices are being enforced.

Task Description: The connection of an individual system to a network requires assurance that the addition of that particular system does not adversely impact the network's security posture. Similarly, assurance is required that users of the network can not adversely impact the system security posture. This subtask examines the system to ensure: 1) the system adheres to the network's security posture by enforcing the network's security rules and procedures, and 2) a system security policy has been defined and is sufficiently enforced to protect the system from unauthorized users or processes attempting access from the network. This subtask examines the system to ensure the system adheres to the network's security policy by enforcing the network's security rules and procedures.

Prerequisite Tasks: Task 1
Suggested Documentation: Security Policy, System Architecture, System Design Specifications, MOAs for connection to external networks/systems, system design review documentation, System CONOPS

Suggested References: *Assessing Controlled Access Protection* (NCSC-TG-028), A *Guide to Understanding Design Documentation in Trusted Systems* (NCSC-TG-007), *Trusted Network Interpretation* (NCSC-TG-005*)*, *Trusted Network Interpretation Environments Guideline* (NCSC-TG-011), *Security for Dial-up Lines* (NBS SPEC PUB 500-137), *Security in ISDN* (NIST SPEC PUB 500-189), *Guideline on User Authentication Techniques for Computer Network Access Control* (FIPS PUB 83), *General Security Requirements for Equipment Using the Data Encryption Standard* (FIPS PUB 140)

Type 2 Level of Effort: Identify all external network connections and determine security features of those networks. System interfaces with network(s) or other systems should be analyzed for compliance with the security connection rules. The system CONOPS should be examined to determine all the connections and interfaces intended for the system. It is also important to determine if there are additional connections planned that are not cited in the initial architecture but will be added after the system's initial fielding. The interface to the network(s), or to other systems, should be analyzed so that the security of systems and networks at both ends of the interface will be maintained.

Type 3 or Type 4 Level of Effort: Identify all external network connections, determine security features and weaknesses of those networks, and analyze the ability of the system to prevent and/or identify security violations caused by these external connections. System interfaces with networks or other systems should be analyzed for compliance with the security connection rules. The system CONOPS should be examined to determine all the connections and interfaces intended for the system. It is also important to determine if there are additional connections planned that are not cited in the initial architecture but will be added sometime after the system's initial fielding. The interface to the network(s), or to other systems, should be analyzed so that the security of systems and networks at both ends of the interface will be maintained. The system design should be examined to verify the interfaces comply with the connection rules.

Task 2: Identify TCB Boundary

Task Objective: Identify the mechanisms in the computer system(s) that are responsible for enforcing or could circumvent the security policy. (Note, this concept of a TCB extends beyond the TCB view defined in the Trusted Product Evaluation Process to include all elements of the system or network within the accreditation boundary.)

Task Description: If the computer product has been evaluated by NSA and is listed on the Evaluated Products List (EPL), the TCB has already been identified for the generic system. The certification team will need to examine the software applications and non-evaluated hardware required on the operational system to determine if the TCB has been extend with these additions. If the computer system has not been previously evaluated, the certification team will need to determine the TCB and its boundary in the same manner as determining if the TCB has been extended. Each software component on the operational system must be examined to determine if it belongs to the TCB, and therefore must be trusted. When examining the component, the certification team must answer the following questions:

- Does the component play a role in enforcing/supporting the security policy (e.g., the DAC mechanism)?

- Can the component circumvent the security policy, or interfere or tamper with the correct operation of the TCB (e.g., processes that run in the privilege state)? If the answer to either of these questions is yes, then the product must be considered part of the TCB and should be a trusted component.

Once the TCB has been identified, the external interfaces must be determined. The functional testing should focus on the security-relevant aspects of the external interfaces. An interface is considered external to the TCB if that interface can be invoked by a subject outside the boundary of the TCB. This determines the boundary of the TCB. Examples of such interfaces are trusted commands, trap or gateway instructions that implement system calls, and libraries that are shared (dynamically linkable) between users and the TCB.

Prerequisite Tasks: Task 1

Suggested Documentation: FER, System Security Architecture, source code, DTLS, FTLS, system design review design documentation (internals of the system design)

Suggested References: *Trusted Database Management System Interpretation* (NCSC-TG-021), *Assessing Controlled Access Protection* (NCSC-TG-028), Guideline for Computer *Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority*

Scheme for EDP Audit and Computer Security Review (NBSIR 86-3386)

Type 3 Level of Effort: Identify the security-critical components of the system, analyze how the TCB supports the system security architecture, and identify the capabilities of the TCB to protect itself from unauthorized usage.

Type 4 level of Effort: Identify the security-critical components of the system at the lowest level possible (e.g., module or board level), analyze the TCB support of the system security architecture, and identify the capabilities of the TCB to protect itself from unauthorized usage.

Task 3: Software, Hardware, Firmware Architecture Study

Task Objective: Map the security policy and requirements to the system software, hardware, and firmware architecture and design.

Task Description: Trace security requirements to the software, hardware, and/or firmware architecture and design. Determine that each security requirement has been implemented to completely and sufficiently perform the required security functions. Examine the source code of the TCB and compare it to the system design documentation and ensure it accurately reflects how the software is written. Ensure that sound software engineering practices were used in the development/maintenance of the TCB software. If evaluated products are used, the team should only review any additional developed security critical source code.

Prerequisite Tasks: Task 1, Task 2, SubTask 3a

Suggested Documentation: Source code, DTLS, FTLS, System Design Specifications, System design review documentation

Suggested References: *Trusted Database Management System Interpretation* (NCSC-TG-021*), Assessing Controlled Access Protection* (NCSC-TG-028), A *Guide to Understanding Design Documentation in Trusted Systems* (NCSC-TG-007), *A Guide to Understanding Object Reuse in Trusted Systems* (NCSC-TG-018), *A Guide to Understanding Discretionary Access Control in Trusted Systems* (NCSC-TG-003), *A Guide to Understanding Audit in Trusted System* (NCSC-TG-001), A *Guide to Understanding Identification and Authentication in Trusted Systems (*NCSC-TG-017), *Trusted Network Interpretation Environments Guideline (NCS*C-TG-011), Trusted Network Interpretation (NCSC-TG-005), *Software Engineering Institute Maturity Model* (FPS PUB 102), *Guideline for Computer Security Certification and Accreditation* (FPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451*)*, *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority*

Scheme for EDP Audit and Computer Security Review (NBSIR 86-3386)

Type 3 level of Effort: Conduct detailed software, hardware, and firmware design and software/firmware code analysis as necessary to determine that each requirement has been completely and correctly implemented. Examine a reasonable sample of the TCB source code (e.g., 40%) for design consistencies and malicious code. If problems/inconsistencies are found, the percentage of code examined should increase.

Type 4 Level of Effort: Conduct detailed software, hardware, and firmware design and software/firmware code analysis as necessary to determine that each requirement has been completely and correctly implemented. Examine a reasonable sample of the TCB source code (e.g., 60%) for design consistencies and malicious code. If problems/inconsistencies are found, the percentage of code examined should increase.

SubTask 3a: Software Engineering Analysis

Task Objective: Ensure the developer/maintainer is using sound and proven development approaches, engineering environment, system analysis and design methodologies, coding standards, and software modularity techniques.

Task Description: Review the developer/maintainer's software engineering discipline, development approach, and engineering environment to analyze whether its use is likely to result in a system that meets the system architecture requirement. During the code studies, the team will compare the implementation to the system described in the design documentation and determines whether the software engineering discipline is reflected in the implementation. In analyzing the modularity of the software, the certification team may analyze the strengths of attributes that may be indicative of modularity and software quality. The following is a non-comprehensive list of these attributes [19]:

- Code cohesion
- Complexity
- Coupling
- Data cohesion
- Duplicate code and data
- Extraneous code and data
- Reliability
- Correctness
- Verifiability

Coding standards, the principles by which the code is written, are usually part of the documentation of the software engineering process, and they may support both the configuration management and system architecture requirements. The analysis should include [19]:

- A description of restrictions on the size of modules
- A description of the rules for using mechanisms that support least privilege
- A review of the rules and conventions governing the selection of identifiers (variables, parameters, filenames)
- A justification for the languages chosen
- The interface constraints and standards that describe a form and style for interfaces in the TCB
- The standard forms and styles for handling initialization and termination conditions, and error recovery and exception handling
- The peer review of the software modules (e.g., design consistency, malicious code)

Prerequisite Tasks: Task 1, Task 2

Suggested Documentation: Software Development Plan, System Development Standards, Source code, DTLS, FTLS, System Design Specifications, system design review documentation

Suggested References: *A Guide to Understanding Design Documentation in Trusted System* (NCSC-TG-007), *Trusted Computer System Architecture: Assessing Modularity*

Type 3 and Type 4 Level of Effort: Examine the development approach and engineering, environment to determine if it is being used correctly. Examine a suitable portion of the security-critical design and code to determine that the engineering environment accurately reflects the implementation of the security requirements. Examine 20% of the security-critical source code to determine if the system development standards were followed (this action may be coupled with the review of the code in Task 3).

Task 4: Interface Analysis

Task Objective: Identify interfaces into the system components.

Task Description: With the increased use of COTS products, the interfaces between the various components of the system become a critical area. Although standards exit, each vendor may have a slightly different method of implementing the appropriate standards. This task must be repeated if technical counter-measures are implemented after this task has been completed.

Prerequisite Tasks: Task 1, additional for Type 3 or 4; Task 2, Task 3

Suggested Documentation: FER, System Security Architecture, source code, DTLS, FTLS, system design review documentation

Suggested References: *Trusted Database Management System Interpretation* (NCSC-TG-021), *Assessing Controlled Access Protection* (NCSC-TG-028), *Trusted Network Interpretation Environments Guideline* (NCSC-TG-011), *Trusted Network Interpretation* (NCSC-TG-005), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority Scheme for EDP Audit and Computer Security Review* (NBSIR 86-3386)

Type 2 Level of Effort: Analyze each external network and/or external system interface, identified in Task 1, to ensure that it enforces the Security Policy and the MOA.

Type 3 Level of Effort: Analyze each external network and/or external system interface, identified in Task 1, to ensure that it enforces the Security Policy and the MOA. Identify the external interfaces to the TCB. Determine which interfaces are used by non-TCB modules to access the TCB.

Type 4 Level of Effort: Analyze each external network and/or external system interface, identified in Task 1, to ensure that it enforces the Security Policy and the MOA. Identify the external interfaces to the TCB. Determine which interfaces are used by non-TCB modules to access the TCB. Determine that the TCB only uses external interfaces to access non-TCB modules or TCB modules in a distributed TCB architecture. Ensure that all references between subjects and objects are mated by a reference monitor.

Task 5: Covert Channel Analysis

Task Objective: Determine if any covert channels exist and identify their maximum attainable bandwidth. Once covert channels have been identified, their bandwidth should be reduced to an acceptable level per the security policy.

Task Description: Ensure that no unintended/unauthorized communications paths exist that violate the security policy. The certification team should focus on the identification of one or more of the following: (1) illegal information flows in top-level design specifications and source code, (2) identification of shared TCB components, (3) state transition analysis of the TCB [20], and (4) changes implemented to the system to reduce the bandwidth of each channel.

Prerequisite Tasks: Task 1, additional for Type 3 or 4; Task 2

Suggested Documentation: Architecture study, DTLS, Security Policy, Formal Security Model, source code, system design review documentation

Suggested References: *C. R. Tsai, V. D. Gligor, and C. S Chandersekaran, A Formal Method for the Identification of Covert Storage Channels in Source Code* (IEEE- Transactions on Software Engineering, 16:6, pp. 569-580, June 1990)*, J. He and V. D. Gligor, Information Flow Analysis for Covert-Channel Identification in Multilevel Secure Operating Systems* (proceedings of the 3rd IEEE Workshop on Computer Security Foundations, Franconia, New Hampshire, pp. 139-148, June 1990)*, K. Loepere, Resolving Covert Channels within a B2 Class Secure System, Operating Systems Review* (ACM SIGOPS, 19:3, pp. 9-28, July 1985)

Type 2, 3, or 4 Level of Effort: Use task objective and description for level of effort.

Task 6: Composition Analysis

Task Objective: Ensure that the integrity of each product and its trusted interfaces are maintained when interfacing to other products in the system.

Task Description: Analyze the impact on each product of combining it with the other products that are part of the system. This task must be repeated if technical countermeasures are implemented after this task has been completed.

Prerequisite Tasks: Task 1, Task 4, additional for Type 3 or 4; Task 2, Task 3

Suggested Documentation: Security Policy, architecture study, Interface Description Document, FER, product/system profiles (if they are available), system design review documentation

Suggested References: *Trusted Network Interpretation* (NCSC-TG-005), *Computer Security, Subsystem Interpretation* (NCSC-TG-009), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451*) Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority Scheme for EDP Audit and Computer Security Review* (NBSIR 86-3386)

Type 2 Level of Effort: Analyze the interfaces at the system level.

Type 3 Level of Effort: Analyze the interfaces at the subsystem level and determine that the interfaces are well bounded with respect to the information flows.

Type 4 level of Effort: Analyze the interfaces at the critical module level, determine that the interfaces are well bounded with respect to the information flows, and ensure that module isolation is maintained when interfaced.

4.1.2.2 Life- Cycle Analysis

There are several ways to ensure life-cycle assurance and they must build on each other in order to achieve the final goal of assuring the security features are implemented properly. Life-cycle assurance provides the overall structure, but INFOSEC analysis, verification, and testing provide the specifics. INFOSEC analysis is the primary way to determine if the requirements are analyzed and documented properly. Validation that the specifications have been implemented properly may be accomplish by various methods (e.g., analysis, demonstration, inspection) depending on the system and degrees of assurance required.

Configuration management is a process for controlling all changes to a system (software, hardware, firmware, documentation, support/testing equipment, development/maintenance equipment). The PM should establish a CCB to review and approve changes to the system. This process should begin as soon as the system's requirements are approved and continue until the system is retired or replaced. There are several reasons for performing life-cycle assurance:

- A baseline be established at a given point in the system life-cycle.

- Systems evolve over time and do not remain static.

- Contingency planning must be addressed for catastrophes (natural or human).

- The use of the system■s finite set of resources will grow through the system■s life-cycle.

- The purpose of these reviews is to ensure that changes control and configuration management practices are in place to preserve the integrity of the system.

Task 7: Configuration Management Plan Review/Audit

Task Objective: Determine if appropriate confirmation management controls have been implemented for the operational system and baselines are established and maintained.

Task Description: Determine that an appropriate level of control has been established to ensure adequate, but not overly restrictive, controls are in place. All personnel making changes to the system must be cleared to the proper security level. For systems requiring a high degree of assurance for confidentiality and integrity, changes to the TCB should be separately controlled. TCB following tasks should be performed for systems requiring medium to high degrees of assurance:

- Configuration item identification
- Configuration control
- Configuration accounting
- Configuration auditing (e.g., malicious code review)
- Trusted distribution

Prerequisite Tasks: Task 1, Task 19; additional for Type 3 or 4; Task 3

Suggested Documentation: CM Plan, System Development Standards

Suggested References: *A Guide to Understanding, Configuration Management in Trusted Systems* (NCSC-TG-006), A *Guide to Understanding Trusted Facility Management* (NCSC-TG-015), *Rating Maintenance Phase Program Document* (NCSC-TG-013), *A Guide* to *Understanding Trusted Distribution in Trusted Systems* (NCSC-TG-008), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life -Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work- Priority Scheme for EDP Audit and Computer Security* (NBSIR 86-3386)

Type 2 Level of Effort: Determine if a CM Plan has been developed and is being followed. Determine that all personnel allowed to change the system configuration have been cleared to the proper level and only approved changes are being implemented on the system.

Type 3 Level of Effort: Determine if a CM Plan has been developed and is being followed. Determine that all personnel allowed to change the system configuration have been cleared to the proper level and only approved changes are being implemented on the system. Determine that CIs are being identified at the appropriate levels. Perform a Physical Configuration Audit (PCA) and Functional Configuration Audit (FCA) of the security components of the system. Review changes to the TCB for malicious code.

Type 4 Level of Effort: Determine if a CM Plan has been developed and is being followed, that security concerns are addressed during the analysis of the system, and all changes to security critical components (e.g., TCB) are strictly controlled and tested. Determine that all personnel allowed to change the system configuration are cleared to the proper level and only approve changes are implemented on the system.

Determine that CIs are being identified at the appropriate levels and that TCB components are separate CIs. Perform a PCA and FCA of every system component. Review changes to the TCB for malicious code.

Task 8: Developmental Suite Configuration Management Review

Task Objective: Determine that the developer has followed an approved configuration management plan for the system used to develop the software and baselines are established and maintained.

Task Description: If the developer is using a separate suite of equipment for development/maintenance, effective configuration management must be implemented. Since the development/maintenance system may be geographically separated from the operational system and its CCB, strict controls should be implemented to ensure the correct configuration of the development/maintenance system. All changes to the development/maintenance system must be approved by the operational site CCB.

Prerequisite Tasks: Task 1, Task 2, Task 7, Task 19

Suggested Documentation: CM Plan, System Development Standards

Suggested References: *A Guide to Understanding Configuration Management in Trusted Systems* (NCSC-TG-006), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102),*Guide to Auditing for Controls and Security : A System Development Life-Cycle Approach* (NBS SPEC PUB 500)0-153), *U.S. Department of Commerce Methodology Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security, Accreditation Guidelines* (NBSIR 4378), *Work Priority Scheme for EDP Audit and Security Review* (NBSIR 86-3386)

Type 3 Level of Effort: Determine that the developer has followed an approved configuration management plan and that the development system is in the approved configuration.

Type 4 level of Effort: Determine that the developer has followed an approved configuration management plan and that the development system is in the approved configuration. The certification team should perform a periodic configuration audits of the developer's site and development system to ensure that the developer has followed the CM Plan.

4.1.2.3 Testing

Testing is the most traditional method of demonstrating that a system functions correctly. Unfortunately, there is truth in the familiar observation that testing only documents the presence of errors, not their absence. One cannot know that a particular error has been made (or not made) unless one tests for it, and there is no way of ensuring that a testing program covers every possible kind of error. The more complex a system, the harder it is to devise thorough tests because the number of possible sequences of operation for even a small program can be enormous [20]. Testing is one of the four methods (i.e., testing, analysis, inspection, demonstration) to verify that a requirement has been correctly implemented. The certification team should be aware of all system testing and review the test plans and procedures to ensure security requirements are addressed. At the completion of any test, the certification team should obtain and review the test report. For systems that have been deployed at multiple locations, several of the testing tasks may need to be performed as part of Activity 5 discussed in Chapter 5. This may include tasks #13, #14, #15, #16, #17, #18, #19, and #20. The CA should prepare the certification package with the caveat that the Accreditor's staff must complete the tasks specified in the certification package.

Task 9: Coverage Analysis of Test Suite

Task Objective: Determine if the test plans and procedures address all the security requirements and the results of the testing will provide sufficient evidence of any risks from operating the system.

Task Description: Review the test plans and procedures to ensure security requirements are tested along with all the interfaces to the TCB.

Prerequisite Tasks: Task 1, Task 4, Task 7, Task 10, Task 19, additional for Type 3 or 4; Task 2, Task 3, Task 8

Suggested Documentation: Security Policy, PCA, Test Plans/Procedures, unit test folders, TCB (boundary and interfaces), DTLS

Suggested References: *DoD-STD-2167A, DoD-STD-7935A, Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority Scheme for EDP Audit and Computer Security Review* (NBSIR 86-3386)

Type 2 Level of Effort: Determine that all the security requirements identified in Task 10 have a corresponding test procedure.

Type 3 Level of Effort: Determine that all the security requirements identified in Task 10 have a corresponding test procedure. All security relevant TCB interfaces identified in Task 2 should also have a corresponding test procedure.

Type 4 Level of Effort: Determine that all the security requirements identified in Task 10 have a corresponding test procedure. All security-relevant TCB interfaces identified in Task 2 should also have a corresponding test procedure. This test should focus testing on the DTLS.

Task 10: Requirements Traceability

Task Objective: Determine that the test plans and procedures cover all the security requirements of the security policy and system specifications.

Task Description: Review the test plans/procedures to ensure they adequately address the security requirements.

Prerequisite Tasks: Task 1, Task 4, Task 7, Task 19, additional for Type 3 or 4; Task 2, Task 3, Task 8

Suggested Documentation: Security Policy, Test Plans/Procedures, unit test folders, requirements traceability matrix, system specifications, System Development Standards

Suggested References: *Johnson Space Center Manual 25285, DoD-STD-7935A, MIL-STD-483, MIL-STD-490, Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certification Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority Scheme for EDP Audit and Computer Security Review* (NBSIR 86-3386)

Type 2 Level of Effort: Determine that tests have been developed to test the correct implementation of the security policy.

Type 3 or Type 4 Level of Effort: Determine that tests have been developed to test the correct implementation of the security policy. Tests should be included to ensure the system responds properly to incorrect input (e.g., system remains in a secure state).

Task 11: Security Functional Testing

Task Objective: Validate that the system provides the required security features. If the system connects to a network or another system, ensure that the security of both ends is being maintained.

Task Description: Hands-on testing should focus on TCB interfaces, system initialization, shutoff, and aborts, ensuring that the system remains in a secure state. Because it is not feasible to include every possible input when testing a system, the tester tries to select those inputs that exercise every module or every system function and place stress on the system. The tester will start with inputs that will demonstrate that the module or system meets each requirement. Errors should be introduced to demonstrate whether the system fails to perform its function when given invalid commands [20]. If network connections are being used, the team should verify that the connection rules are enforced.

Prerequisite Tasks: Task 1, Task 4, Task 7, Task 9, Task 10, Task 11 a, Task 19, additional for Type 3 or 4; Task 2, Task 3, Task 8

Suggested Documentation: System Design Specifications, Requirements Traceability Matrix, Test Plans/Procedures, Security Policy, SFUG, Operating Instructions (OIs), TFM, Security CONOPS, Network Connection Rules, MOAs

Suggested References: *Assessing Controlled Access Protection* (NCSC-TG-028) *Guide to Understanding Trusted Facility Management* (NCSC-TG-015), *A Guide to Writing the Security Features User's Guide for Trusted Systems* (NCSC-TG-026), *A Guide to Understanding Object Reuse in Trusted Systems* (NCSC-TG-018), A *Guide to Understanding Discretionary Access Control in Trusted Systems* (NCSC-TG-003), *A Guide to Understanding Audit in Trusted Systems* (NCSC-TG-001), *A Guide to Understanding Identification and Authentication in Trusted System* (NCSC-TG-017), A *Guide to Understanding Trusted Recovery in Trusted Systems* (NCSC-TG-022), *Guideline for Computer Security Certification and Accreditation* (FPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U..S. Department of Commerce Methodology Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority Scheme for EDP Audit and Computer Security Review* (NBSIR 86-3386)

Type 2 Level of Effort: Determine that the high-level requirements of the security policy have been implemented. Validate the correctness of the TFM and SFUG. Validate the compliance with the network connections rules.

Type 3 Level of Effort: Determine that the high-level requirements of the security policy have been implemented. Validate the correctness of the TFM and SFUG. Analyze the strengths/ weaknesses of I&A, audit, and access controls (e.g., MAC and DAC). Validate the compliance with the network connection rules and analyze the effectiveness of these security features.

Type 4 Level of Effort: Determine that all the requirements of the security policy have been implemented. Validate the correctness of the TFM and SFUG. Analyze the strengths/ weaknesses of object reuse, trusted recovery, I&A, audit and access controls (e.g., MAC, DAC, labels). Validate the compliance with the network connection rules and analyze the effectiveness of these security features.

SubTask 11 a: System Test Configuration

Task Objective: Determine that the system configuration (e.g., hardware, software, firmware, documentation) adequately represents the operational system and the test results obtained from using the test suite will reflect the performance of the operational configuration. If generic test data is used to exercise the system, the certification team should analyze how accurately the test data represents actual data from the operational system.

Task Description: Review the test suite configuration and ensure that it is a functional representation of the operational system and that the correct CIs are used.

Prerequisite Tasks: Task 1, Task 4, Task 7, Task 9, Task 10, Task 19, additional for Type 3 or 4; Task 2, Task 3, Task 8

Suggested Documentation: Security Policy, PCA, CM Plan, test plans/procedures, unit test folders

Suggested References: *A Guide to Understanding Configuration Management in Trusted Systems* (NCSC-TG-006)

Type 2 level of Effort: Determine that the same type of components have been used for the test and operational system.

Type 3 level of Effort: Determine that the same type of components have been used for the test and operational system and that the test system is at least a functional representation of the operational system.

Type 4 Level of Effort: Determine that the same type of components have been used for the test and operational system and that the test system is at least a functional representation of the operational system. Ensure that results obtained from the test system will reflect the performance of the operational system.

Task 12: Reliability Testing

Task Objective: Validate that the system meets the required reliability.

Task Description: Obtain the hardware and software failure reports and determine the reliability of each critical component. This data may be obtained from the operational system (if it is an existing system), from the development agency (for a new system), or from the vendor (for COTS products).

Prerequisite Tasks: Task 1, Task 4, Task 7, Task 19, additional for Type 3 or 4; Task 2, Task 3

Suggested Documentation: System Design Specifications, System/Component Reliability Data, Test Plans/Procedures

Suggested References: *MIL-HDBK-217E, MIL-STD-785B, Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), Guide to Auditing for Controls and Security: *A System Development Life-Cycle Approach (NBS* SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378)*, Work Priority Scheme for EDP Audit and Computer Security Review* (NBSIR 86-3386)

Type 2 Level of Effort: Review the system/component reliability data and determine if the security components meet the required component reliability.

Type 3 Level of Effort: Review the system component reliability data and determine if the security components meet the required component and system reliability.

Type 4 level of Effort: Review the system component reliability data and determine if the security components meet the required component and system reliability. Determine that the system meets the reliability requirements in the operational environment.

Task 13: Penetration Testing

Task Objective: Circumvent the system security features.

Task Description: Penetration testing includes reviewing all system design and implementation documentation (e.g., system source code, manuals, and communications diagrams and hands-on testing. When performing this testing, the certification team should work under no constraints [21] and should have complete hands-on access to the system. Although a penetration test plan should be developed, it should allow for flexibility if weaknesses in the system are found. A team of individuals who are familiar with the system being tested and with typical flaws in protection systems should attempt to defeat the protection mechanisms of the system. The technics used are both analytic and intuitive. First, flaws are hypothesize and tested. If these flaws materialize, they are extended to try to defeat more components of the system. In this way, the penetration testers should try to operate as would an intruder intent on defeating the protection mechanisms of the system [20].

Prerequisite Tasks: Task 1, Task 4, Task 7, Task 19, additional for Type 3 or 4; Task 2, Task 3, Task

8

Suggested Documentation: System Design Specifications, System/Component Reliability
Data, Test Plans/Procedures/Reports, Security Policy, SFUG, OIs, TFM, system vulnerabilities, System Architecture Study, source code, Network Connection Rules, MOAs

Suggested References: *Assessing Controlled Access Protection* (NCSC-TG-028), *A Guide To Writing the Security Features User's Guide for Trusted Systems* (NCSC-TG-026), *A Guide to Understanding Object Reuse in Trusted System* (NCSC-TG-018), *A Guide to Understanding Discretionary Access Control in Trusted Systems* (NCSC-TG-003), *A Guide to Understanding Audit in Trusted Systems (*NCSC-TG-001*), A Guide to Understanding Identification and Authentication in Trusted Systems* (NCSC-TG-017)

Type 2 Level of Effort: Look for obvious flaws (e.g., vendor-installed passwords, errors in the SFUG and TFM). For network connections, try to circumvent the network connections.

Type 3 or Type 4 Level of Effort: Look for obvious flaws (e.g., vendor-installed passwords, errors in the SFUG and TFM). Generate hypothesis on system flaws. After generating a list of possible penetrations, tools and/or code may be needed to exploit these flaws. It is recommended that additional time and staffing be used for a Type 4 certification. For network connections, try to circumvent the network connection rules.

Task 14: TEMPEST Testing

Task Objective: Determine the TEMPEST requirements, if any, of the facility in which the system is to be installed. Proper zoning of the system components is the major focus of this task.

Task Description: NSTISSI 7000 identifies which facilities require a review of the TEMPEST posture. It states that a Certified TEMPEST Technical Authority (CTTA) must conduct or validate all TEMPEST countermeasure reviews.
In conducting TEMPEST countermeasure reviews, the CTTA should consider the location of the facility, the sensitivity and perishable nature of the information processed, the physical control over the facility, and the TEMPEST profile of equipment. However, the requirement to conduct or validate a review does not necessarily imply the need to implement countermeasures. When it is necessary to implement TEMPEST countermeasures, the most cost-effective countermeasure will be used.

The most cost-effective way to meet TEMPEST countermeasure requirements will often be TEMPEST zoning. However, when zoning is not appropriate, other countermeasures may be appropriate, such as the installation of radio frequency shielding the installation of foil backed wallboard or the use of EST suppressed equipment. Also, RED/BLACK installation criteria may necessary.

Prerequisite Tasks: Task 1, Task 4, Task 7, Task 19, additional for Type 3 or 4; Task 2, Task 3, Task 8

Suggested Documentation: TEMPEST Review Report

Suggested References: *NSTISSP No. 300, NSTSSI 7000, NSTISSAM TEMPEST 12-92, NSTISSAM TEMPEST 11 -92, NACSEM 5203*

Type 2 Level of Effort: Determine if zones have been established and generic equipment types are in the proper zones.

Type 3 Level of Effort: Determine if zones have been established and generic equipment types are in the proper zones, and identify the zone rating of each piece of equipment.

Type 4 Level of Effort: Determine if zones have been established and generic equipment types are in the proper zones, and identify the zone rating of each piece of equipment, and review the cable separation plan and facilities capability. In some cases, an instrumented test may necessary.

Task 15: COMSEC Testing

Task Objective: If COMSEC testing is required, test the implementation and interactions of the cryptographic components of the system. Key management and physical protection of the COMSEC equipment is the major focus of this task.

Task Description: A cryptographic system's defenses against standard attacks are centered in the algorithm, the key management, and the automated cryptographic security and automated alarms. Cryptographic systems can be attacked through cryptoanalysis, theft of cryptographic components, and exploitation of user or system errors [21].

The Achilles heel for performance in systems with embedded cryptographic components is key management. The final key management design is affected by [28]:

- The operational and security environment
- The availability of manual or electronic delivery system
- The availability of qualified people
- The reliability and speed of communications
- The need for transparency
- The possible need for emergency bypass features

Prerequisite Tasks: Task 1, Task 4, Task 7, Task 15, Additional for Type 3 or 4; Task 2, Task 3, Task 8

Suggested Documentation: Tailored Functional Security Requirements Specification (FSRS) - classified

Suggested References: *NACSI No. 4005, Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB ????53), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guideline* (NISTIR 4378), *Work Priority Scheme for EDP Audit and Computer Security Review* (NBSTIR ??6-3386), *Public-Key Cryptography* (NIST SPEC PUB 800-2), *Maintenance Testing for ?? Data Encryption Standard* (NBS SPEC PUB 500-61), *Key Management Using ANS??17* (FIPS PUB 171)

Type 2 Level of Effort: Review the key management plan for existence and completeness.

Type 3 Level of Effort: Review the key management plan for existence and completeness and review the key handling procedures.

Type 4 Level of Effort: Review the key management plan for existence and completeness and review the key handling procedures. Audit the use of the key handling procedure by operations personnel.

Task 16: Contingency Plan Testing

Task Objective: Ensure that the continency plan addresses all known risks to the system and is current, complete, and is tested. These risks include:

- Natural risks (fire, storms, earthquakes)
- Environmental risks (water, steam, power, air conditioning)
- Security risks (system failure, security violation)

Task Description: These procedures specify the steps and actions to be taken to protect life and property and to minimize the impact of the contingency. Since there will always be risks associated with any computer system, backup and recovery plans are a necessity. A contingency plan contains the procedures for backing up critical applications and hardware, and procedures to recover quickly from an unforeseen disaster for which no safeguard was implemented, the safeguard failed, or was bypassed. The team should review the Risk Analysis Report and identify emergency conditions that impact system operation. A contingency plan should at least cover the following items:

- Emergency response procedures
- Backup operations
- Recovery procedures
- Plan maintenance
- Preparatory actions
- Testing
- Critical applications identification
- Critical resources identification

Prerequisite Tasks: Task 1, Task 7, Task 9, Task 17, Task 18, Task 19, Task 20, additional for Type 3 or 4; Task 8

Suggested Documentation: Risk Analysis Report, OIs, contingency plan.

Suggested References: A *Guide to Understanding Trusted Facility Management* (NCSC-TG-015), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Authorized Information* System *Security Accreditation Guidelines* (NISTIR 4378), *Work Priority Scheme for EDP Audit and Computer Security Review (*NBSIR 86-3386), *Guide on Selecting ADP Backup Process Alternatives* (NBS SPEC PUB 500-134), *Guidelines for ADP Contingency Planning* (FIPS PUB 87), *Executive Guide to ADP Continency Planning* (NBS SPEC PUB 500-85), *Domestic Disaster Recovery Plans for PCS, OIS, and Small VS Systems* (NISTIR 4359)

Type 2 Level of Effort: Determine that a contingency plan has been developed and covers the risks listed in the task objective, the items listed in the task description, and individuals are trained in the proper procedures.

Type 3 Level of Effort: Determine that a contingency plan has been developed and covers the categories list in the task objective, the items listed in the task description, individuals are trained in the proper procedures, and where possible, the procedures are actually tested (e.g., no simulation).

Type 4 Level of Effort: Determine that a continency plan has been developed and covers the risks listed in the task objective and the items listed in the task description. To ensure individuals are trained in the proper procedures, all the procedures are tested in some fashion, and the contingency plan satisfies the availability, integrity, confidentiality, and accountability requirements of the system.

4.1.2.4 Physical Security Analysis

Physical security includes the application of physical barriers and control procedures as countermeasures against threats to resources and sensitive information. The type of analysis that needs to be conducted in this area is dependent on the classification level of the information to be stored, transmitted, or processed. If all the degrees of assurance are low and a Type I certification is selected, minimal documentation and physical security requirements should be in place. If a Type 4 certification is required, a separated accreditation of the facility may be required (e.g., Sensitive Compartmented Information Facility (SCIF) accreditation). Not all Type 4 certifications imply that a SCIF accreditation is required, but additional documentation and/or inspections may be required to verify the physical security requirements have been met.

Task 17: Facility Perimeter Analysis

Task Objective: Determine if access to the facility, computer room, terminal areas, media storage, communications switches, and printer areas, for example, are adequately controlled.

Task, Description: The level of physical protection should be commensurate with the degree of assurance for availability and integrity needed and the classification of data processed.

Prerequisite Tasks: Task 19

Suggested Documentation: OIs, Security Policy, Police Surveys, Threat Surveys

Suggested References: A *Guide to Understanding Trusted Facility Management* (NCSC-TG-015), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR4451), *Automated lnformation System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority Scheme for EDP Audit and Computer Security Review* (NBSIR 86-3386)

Type 2 Level of Effort: Analyze the physical access controls of the critical AIS facilities.
Physical penetrations should be attempted.

Type 3 Level of Effort: Analyze the physical access controls of the critical AIS facilities, media storage, communications switches, printer areas, and terminal areas. Physical penetrations should be attempted.
Type 4 Level of Effort: Analyze the physical access controls of the critical AIS facilities, media storage, all communications switches, all printer areas, and all terminals areas. Physical penetrations should be attempted.

Task 18: Environmental Control Analysis

Task Objective: Determine if the environmental controls (e.g., fire suppression, water and fire sensors, HVAC, power availability) meet the requirements for processing.

Task Description: The level of environmental protection should be commensurate with the degree of assurance needed for availability. If there is a requirement for a high degree of assurance for availability, then the environmental controls should be stringent and system redundancy should be available. Obviously, the environmental controls should be in place no matter what degrees of assurance are required, but the type and amount of these controls may vary if the threat of non-availability or sabotage is low.

Prerequisite Tasks: Task 19

Suggested Documentation: OIs, Security Policy, Fire Inspections, Threat Surveys, Building Inspections, Electrical Surveys

Suggested References: *A Guide to Understanding Trusted Facility Management* (NCSC-TG-015), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work- Priority Scheme for EDP Audit and Computer Security Review* (NBSIR 86-3386)

Type 2 Level of Effort: Determine that safety inspections are current and complete.

Type 3 Level of Effort: Determine that security inspections are current and complete and safety procedures are in place and administrated regularly.

Type 4 Level of Effort: Determine that safety inspections are current and complete, safety procedures are in place and administrated regularly, and the safety systems and procedures have been tested.

4.1.2.5 Operational Security Review

There are many administrative and operational procedures that must be properly implemented prior to the system becoming operational. Individuals must be appointed to various positions and all system users should obtain adequate training. Any countermeasures that were implement to reduce the risk must also be tested for proper installation and effectiveness.

Task 19: Minimal Security Checklist

Task Objective: Determine if the minimum INFOSEC requirements are properly implemented.

Task Description: This task requires completion of the minimal checklist in Appendix F. After the checklist has been completed, a report should be written summarizing the strengths and weaknesses of the system. This report will then form the basis for the accreditation package for Type 1 certifications.

Prerequisite Tasks: None

Suggested Documentation: OIs, Security Policy, SFUG, TFM, Site Survey, CM Plan, Contingency Plan, Fire Survey, Building Survey

Suggested References: *Trusted UNIX Working Group* (TRUSIX) *Rationale for Selecting Access Control List Features for the UNIX System* (NCSC-TG-020-A), *A Guide to Understanding Configuration Management in Trusted Systems* (NCSC-TG-006), *A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems* (NCSC-TG-027), *Assessing Controlled Access Protection* (NCSC-TG-028), *A Guide to Understanding Trusted Facility Management* (NCSC-TG-015), *A Guide to Writing the Security Features User's Guide for Trusted Systems* (NCSC-TG-026), *A Guide to Understanding Discretionary Access Control in Trusted Systems* (NCSC-TG-003), *A Guide to Understanding Audit in Trusted Systems* (NCSC-TG-001), A *Guide to Understanding of Defense Identification and Authentication in Trusted Systems*(NCSC-TG-017), *Department Password Management Guideline* (CSC-STD-002-85), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *U.S. Department of Commerce Methodology for Certifying Sensitive Computer Applications* (NISTIR 4451), *Automated Information System Security Accreditation Guidelines* (NISTIR 4378), *Work Priority Scheme for EDP Au&t and Computer Security Review* (NBSIR 86-3386), *Security for Dial-up Lines* (NBS SPEC PUB *500-137), Guideline on User Authentication Techniques for Computer Network Access Control* (FIPS PUB 83), *Minimum Security Requirements for Multi-User Operating Systems* (NISTIR 5153)

Task 20: Operational Procedure Review

Task Objective: Determine if operational procedures have been established and are being followed by all appropriate users to minimize system security deficiencies and to validate the correctness of the checklist completed in Task 19.

Task Description: For each system risk that an operational countermeasure was implemented to address, the certification team must ensure that the procedure has been implemented correctly, reduces the risk to the specified level, and is being followed by all appropriate system users. For each operational procedure, determine that all users have been properly trained. If technical countermeasures are implemented after Tasks 4 and 6 are completed, these two tasks must be repeated for the technical countermeasures.

Prerequisite Tasks: For Type 1; Task 19, additional for Types 2, 3, and 4; Task 1, Task 4, Task 10, Task 13, Task 14, Task 15, Task 16, Task 17, Task 1 8, additional for Types 3 or 4; Task 2, Task 3, Task 8

Suggested Documentation: OIs, Security Policy, SFUG, TFM, Risk Analysis Report

Suggested References: *A Guide to Understanding Trusted Facility Management* (NCSC-TG-015), *A Guide to Writing the Security Features User's Guide for Trusted Systems* (NCSC-TG-026), *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), *Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach* (NBS SPEC PUB 500-153), *Security for Dial-up Lines* (NBS SPEC PUB 500-137), *Guideline on User Authentication Techniques for Computer Network Access Control* (FIPS PUB 83), *Minimum Security Requirements for Multi-User Operating Systems* (NISTIR 5153)

Type 1 or 2 Level of Effort: For this type of certification, the Accreditor may rely on more operational procedures to reduce the risks. For each risk that an operational procedure was developed to address, the certification team should determine that a procedure exists, users have been trained, the procedure has been tested and reduces the risk to an acceptable level. Perform spot checks on 10% of the users to determine if they have been adequately trained in the operational security procedures.

Type 3 Level of Effort: For this type of certification, the Accreditor may not rely as heavily on operational procedures to reduce the risks. For each risk that an operational procedure was developed to address, the certification team should determine that a procedure exists, users have been trained, the procedure has been tested and reduces the risk to an acceptable level. Performing spot checks on 30% of the users to determine if they have been adequately trained in the operational security procedures. For risks which technical countermeasures have been implemented, ensure that the countermeasure has been installed correctly, users have been properly trained, and risks have been reduced to the specified level. The certification team should determine if the reliance placed on each of the countermeasures has been justified. The interdependencies between the various countermeasures should be reviewed to ensure that one countermeasure does not impact the effectiveness of another countermeasure.

Type 4 Level of Effort: For this type of certification, the Accreditor should not heavily rely on operational procedures to reduce the risks. For each risk that an operational procedure was developed to address, the certification team should determine that a procedure exists, users have been trained, the procedure has been tested and reduces the risk to an acceptable level. Perform spot checks on 60% of the users to determine if they have been adequately trained in the operational security procedures. For risks which technical countermeasures have been implemented, ensure that the countermeasure has been installed correctly, users have been properly trained, and risks have been reduced to the specified level. The certification team should determine if the reliance placed on each of the countermeasures has been justified. The interdependencies between the various countermeasures should be reviewed to ensure that one countermeasures does not impact the effectiveness of another countermeasure.

4.1.3 Conduct Vulnerability Analysis

The vulnerability analysis task is conducted throughout Phase II in conjunction with the other analysis tasks. It is completed at the end of activity 2 to examine all the reported discrepancies, to determine if any vulnerabilities exist, and if so, to evaluate the residual risk from these vulnerabilities. This task is a key function of the ongoing risk management of the system development. As such, it forms the basis for the recommendation to proceed to Phase III.

Task 21 - Vulnerability Evaluation

Task Objective: Evaluate security vulnerabilities of the services providing, confidentiality, integrity, availability, and accountability, evaluate residual risk, and recommend appropriate countermeasures.

Task Description: Analyze each of the vulnerabilities and discrepancies isolated during the course of the System Analysis to determine the ease of exploitation, potential rewards to the exploiter, probability of occurrence, related threat and residual risk. Conduct fault tree or flaw hypothesis (static penetration) analysis to determine the ability to exploit the vulnerabilities discovered during the previous analysis tasks. Determination of the potential rewards to the exploiter shall consider the sensitivity of the data and processes, criticality of system operation, time criticality, ability to recreate the data or processes, etc. The residual risk (that portion of risk that remains after security measures have been applied) should be determined by ranking the evaluate vulnerabilities against threat, ease of exploitation, potential rewards to the exploiter, and a composite of the three areas. All residual risks should be identified and evaluated. The evaluation should indicate the rationale as to why the risk should be accepted or rejected. Appropriate countermeasures should be determined for each of the high risk vulnerabilities.

Prerequisite Tasks: All tasks that apply for the given certification type.

Suggested References: *Guidelines for Automatic Data Processing Physical and Risk Management* (FIPS Publication 31), *Guideline for Automatic Data Processing Risk Analysis* (FIPS Publication 65), *Configuration Management Military Standard* (MIL-STD-973), *Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software* (FIPS Publication 101), *Guideline for*

Computer Security Certification and Accreditation (FIPS Publication 102), *Software Verification and Validation - Its Role in Computer Assurance and Its Relationship with Software Project Management Standards* (NIST Special Publication 500-165), *Automated Tools for Testing Computer System Vulnerability* (NIST Special Publication 800-6), *Systems Engineering Management Guide* (Defense Systems Management College, January 1990), *A Guide to Understanding Audit in Trusted Systems* (NCSC-TG-001), *A Guide to Understanding Discretionary Access Control in Trusted Systems* (NCSC-TG-003), *A Guide to Understanding Configuration Management in Trusted Systems* (NCSC-TG-006), *A Guide to Understanding Design Documentation in Trusted Systems* (NCSC-TG-007), A *Guide to Understanding Trusted Distribution in Trusted Systems* (NCSC-TG-008), *Trusted Network Interpretation Environments Guideline* (NCSC-TG-011), *Rating Maintenance Phase Program Documentation* (NCSC-TG-013), *A Guide to Understanding Trusted Facility Management* (NCSC-TG-015), *A Guide to Understanding Identification and Authentication in Trusted Systems* (NCSC-TG-017), *A Guide to Understanding Object Reuse in Trusted Systems* (NCSC-TG-018), *Trusted Database Management System Interpretation* (NCSC-TG-021), *A Guide to Understanding Trusted Recovery in Trusted Systems* (NCSC-TG-022), *Assessing Controlled Access Protection* (NCSC-TG-028).

Type 2 Level of Effort: This task shall examine the task discrepancy and summary reports and evaluate the vulnerabilities discovered during those evaluations. The criticality of the vulnerabilities shall be assessed and the vulnerabilities rank ordered with respect to ease of exploitation and potential rewards to the exploiter. All results shall be documented and consolidated into a draft certification package. (These results will be consolidated into the certification package in Phase III.)

Type 3 Level of Effort: This task shall examine the task discrepancy and summary reports and evaluate the vulnerabilities discovered during those evaluations. The criticality of the vulnerabilities shall be assessed and the vulnerabilities rank order with respect to ease of exploitation and potential rewards to the exploiter. Countermeasures shall be proposed to offset the risk of each vulnerability. All results shall be documented and consolidated into a draft certification package. (These results will be consolidated into the certification package in Phase III.)

Type 4 Level of Effort: This task shall examine the task discrepancy and summary reports and evaluate the vulnerabilities covered during those evaluations. The criticality of the vulnerabilities shall be assessed and the vulnerabilities rank ordered with respect to ease of exploitation and potential rewards to the exploiter. Countermeasure shall be proposed to offset the risk of each vulnerability. A cost to implement each proposed countermeasures versus risk trade-off analysis shall be performed. All results shall be documented and consolidated into a draft certification package. (These results will be consolidated into the certification package in Phase III.)

4.2 Activity 4 - Report Certification Findings and Recommendations

4.2.1 Complete Certification Package

In order to ensure reusability of the certification evidence, a standard format should be followed for the certification package. The certification team should realize that the certification package, not the accreditation package, will be a major input for recertifying the system. As stated in Chapter 2, this is the final Activity in Phase II of the C&A process. This Activity involves documenting/coordinating the results and recommendations of Activity 3 to prepare the C&A packages. The dates/versions of all documents, policies, and references used in the certification should be included in the package. This will assist in the reunification and make it easy for the team performing the recertification to determine if any of these documents have changed since the last certification was performed.

The certification package is the consolidation of all the previous certification results (testing, analysis). It will be used as supporting documentation for the accreditation decision and will also support recertification/reaccreditation activities. The compilation of the certification package should be done consistently and cost-effectively [1]. If any analysis or testing could not be completed, this limitation should be clearly stated in the package along with the reason why it could not be completed.

The certification package, whether prepared by the Government or the contractor, should contain a set of supporting documents. These documents are necessary since they provide tangible evidence that necessary actions have been completed. The CA should carefully determine the number, scope, and applicability of the documents to match the certification requirements. For larger systems, a certification letter from the CA to the Accreditor may be included. (A sample Certification Letter is included in Appendix K.) The certification package should contain documentation that would not only assist the Accreditor in making the decision to operate, but also assist any future recertification and reaccreditation of this system or a similar system. Appendix I identifies the required contents of the certification package by type of certification. For Type I certifications, the only requirement is completion of the checklists in Appendix F and the accreditation package.

4.2.1.1 Supplemental Documentation

Appendix I also contains a list of supplemental documentation, by type of certification, that may be included in the certification package. The decision to include these additional documents is at the discretion of the CA, but should be based upon the availability of the document and the requirements of the Accreditor. When a document is not applicable, a statement should be included attesting to a document's non-applicability [13]. Although copies of these documents are not normally provided to the Accreditor, their completeness, accuracy, and availability form the basis for reuse of the analysis effort during, recertification or analysis of a similar system.

4.2.1.2 Report of Findings

The report of findings is the primary output of the certification process. It should identify all residual risks and include recommendations concerning the implementation of additional safeguards and approval to operate. This report is produced by the certification team. The certification team is responsible for making a technical judgment of the system's compliance with stated requirements, identifying and analyzing the risks associated with operating the system, coordinating the certfication activities, and consolidating the certfication and accreditation packages. The CA has the opportunity to report certification results to the Accreditor and to explain the potential ramifications of the findings in terms of risks in operating the system [13]. This report should include the recommendation from the CA as to the compliance of the system to the stated security requirements.

4.2.1.3 Classification of Findings

The disclosure of information which, if exploited, could impact the function of a system or allow security features to be bypassed, must be protected from disclosure to unauthorized persons [13]. These findings include, but are not limited to, identification of dual risks and recommendations of the certification team. The certification package must be marked, handled, and controlled consistent with the sensitivity of the information it contains. When possible, classified information should be placed in a separate appendix to the package.

SECTION 5

PHASE III: ACCREDITATION

Accreditation is the official management authorization to operate a system. The Accreditor formally accepts security responsibility for the operation of the system and officially declares that a specified system will adequately protect against denial of service, accountability failure, compromise, destruction, or unauthorized modification under stated parameters of the accreditation. The accreditation decision affixes security responsibility with the Accreditor and shows that due care has been taken for security in accordance with the applicable policies and the Accreditor is willing to accept all risks inherent in operating the system. Since this is the decision of the Accreditor, the CA should not be involved after he/she determined the amount of residual risk.

The accreditation normally grants approval for the system to operate (1) in a particular security mode, (2) with a prescribed set of INFOSEC countermeasures (administrative, physical, personnel, COMSEC, emissions, and COMPUSEC controls), (3) against a defined threat and with stated vulnerabilities and countermeasures, (4) within a given usage concept and environment, (5) with stated interconnections to other systems, (6) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility, and (7) for a specified period of time.

When there are multiple Accreditors, the sharing of responsibilities must be carefully defined in an MOA prior to connection of the separately accredited systems. The Accreditor exercises the prerogative to grant (or deny) authority for a computer system to process actual data in an operational environment. The Accreditor must have the authority to analyze the overall system requirements of the system and to provide definitive directions to system developers or owners relative to the risk in the security posture of the system. Generally, the more sensitive the data processed by a system, the more senior the Accreditor. An Accreditor may be responsible for several systems, and each system may have a single Accreditor or multiple Accreditors.

The Accreditation Phase consists of the following three Activities: (1) Perform Risk Assessment, (2) Report Accreditation Findings and Recommendations, and (3) Make the Accreditation Decision. These three activities are based on information provided to the Accreditor during the Report Certification Findings/Recommendations Activity of the Certification Phase. Conducting a site visit is an optional task that may be deemed necessary by the Accreditor depending on the specific operational environment and threats to counter.

1. Differentiation of security modes is becoming less valuable in considering system security determinations in light of a national security infrastructure that promotes shared resources and network environments. Because of interoperation and interconnections today, most systems are, or are becoming, multilevel secure in some way or another.

5.1 Activity 5 Perform Risk Assessment

Although federal policies may no longer require the preparation of a formal risk analysis, they mandate a risk management program for each AIS. The risk assessment approach should include a consideration of the major factors in risk management: the value of the system, threats, vulnerabilities, and the effectiveness of the countermeasures proposed. Risk management may include an optional site survey, initial risk analysis, cost-benefit analysis, Security Test and Evaluation (ST&E) results, and countermeasures selection and implementation. The outcome is the identification of residual risks. The twofold purpose of conducting a vulnerability assessment and risk analysis is to determine the residual risk that exists for a system and to help the Accreditor understand the risks and their expected impact on the overall mission. Security risks should be addressed throughout the system life-cycle. Management commitment to a comprehensive risk management program must be defined as early as possible in the program life-cycle. In scheduling risk management activities and designating resources, careful consideration should be given to C&A goals and milestones. Associated risks can then be analyzed and corrective action considered for risks that are unacceptable. For each degree of assurance (high, medium, low), different actions should be addressed to lower the risk while considering the cost of the necessary actions. There are some automated risk management tools available and the certfication team should determine if any of them meet the certification team's needs.

5.1.1 Conduct Site Survey (optional)

The site survey may be accomplished by the Accreditor or by local site resources as deemed necessary dependent upon the operational environment. If the system is in a high-risk environment and will process valuable information, then the Accreditor or the accreditation team may wish to inspect the site to verify the constraints of the accreditation have been properly implemented. Although the site survey occurs at a specific point in the C&A process, the Accreditor should routinely survey the site during the certification.

The inspection will include analysis of the technical and nontechnical countermeasures identified in the accreditation package. The purpose of the analysis is to ensure that the countermeasures selected are in place and properly functioning. Task 20 (from Chapter 4) is a starting point for this analysis. The analysis should address administrative, physical, personnel, communications, emission, and computer security disciplines.

5.1.2 Assessment of Vulnerabilities and Associated Risk

The first task of this activity is the performance of a vulnerability assessment and risk analysis.

This task will identify vulnerabilities and associated countermeasures, the costs of each countermeasure, and the amount of residual risk if the countermeasure is or is not implemented. It provides an integrated, comprehensive view of the system combining all the analysis results from each security discipline (from the previous two activities). This analysis considers operational factors and controls that may be in place for the system. Once these factors are considered and the vulnerabilities have been identified through documentation review and testing, the certification team reviews system threats and unique mission requirements. During the INFOSEC analysis, system vulnerabilities may be identified for specific environments.

The subjective assessment of risks associated with employing the system is the basis for accreditation. Each of the vulnerabilities and discrepancies isolated during the evaluation of the system architecture, system design, network interfaces, product integration, and configuration management practices is analyzed to determine its susceptibility to exploitation, the potential rewards to the exploiter, the probability of occurrence, and any related threat. The residual risk, that portion of risk that remains after security measures have been applied, should be determined by ranking the evaluated vulnerabilities against threat, ease of exploitation, potential rewards to the exploiter, and a composite of the three areas. All residual risks should be identified and evaluated. The evaluation should indicate the rationale as to why the risk should be accepted or rejected, and the operational impacts associated the these risks. The results of the assessment should be documented in the accreditation package with the following objectives [13]:

- Identify and analyze any system discrepancies and latent security vulnerabilities discovered in the system analysis.

- Analyze the security risks associated with employing the system. This analysis should address normal usage, degraded usage, and stressed usage.

- Analyze the supporting documentation in terms of completeness, accuracy, and consistency.

- For each vulnerability, recommend countermeasures or analyze the acceptability of the associated risks.

- Identify any limitations or restrictions necessary for acceptable risk when the system is fielded and functioning in the selected security mode of operation. Identify the basis for provisional or interim accreditation, if applicable.

- Document any action items that may impact the accreditation decision.

- Provide conclusions and recommendations based on this analysis.

Task #21 (from Chapter 4) is a starting point for this analysis. The analysis should address all INFOSEC aspects.

5.1.3 Residual Risk

The accreditation team should focus on identifying all residual risks so that steps can be taken to sufficiently reduce the likelihood of the risk(s) occurring. Residual risk is defined as the portion of risk that remains after security measures have been applied [1]. The CA and Accreditor should ensure that any security countermeasures do not introduce additional risks or mitigate other security countermeasures. For each residual risk, the report should contain a residual risk statement specifying the rationale for accepting/rejecting the risk and possible future modifications to resolve the problem. If future solutions are proposed, a tentative implementation schedule and associated cost data should be included in the report. With this type of information provided to the Accreditor, interim approval may be granted pending installation of future modifications.

5.2 Activity 6 Prepare Accreditation Recommendation

Activity 6 involves preparation of the accreditation recommendation and preparation of the accreditation package. The accreditation team should provide recommendations to the Accreditor concerning the type of approval or non-approval to operate the system. It should include an executive summary to include the purpose of the system, degrees of assurance (confidentiality, integrity, availability, and accountability), and the impacts of residual risks. Recommendations can be made to correct deficiencies temporarily or permanently and identify the potential security risk ramifications. Based on the recommendations of *Guideline for Computer Security Certification and Accreditation* (FIPS PUB 102), another recommendation can be to conduct a more detailed certification evaluation in particular areas, whether the current evaluation was inadequate [13]. Accreditation recommendations include:

- Grant full accreditation approval: No restrictions apply. The approval to operate letter should contain information concerning the reaccreditation policy for the system.

- Grant interim (temporary) accreditation approval: Permission to operate might be for a temporary time period or require additional security protection features (e.g., until security feature "X" is corrected, tested, and certified, no information more sensitive than "Y" can be processed) [l]. In some instances, authority to operate might be restricted to a specific operational circumstance or mode (e.g., only during crisis or only in the Dedicated Security Mode) [1].

- Disapprove accreditation: Disapproval, including recommendations and timelines for correcting specified deficiencies.

5.2.1 Caveats

When systems must be operated with major problems, conditional or limited authority may be granted. This is an interim measure only, pending implementation of additional security features. A review schedule and continuing oversight is necessary to ensure conditions of the interim accreditation are adhered to and additional security features to be implemented are not forgotten [13].

5.2.2 Additional Security Features

Several areas should be considered if the system requires additional security protection. Security protection controls may be added, but they will usually be limited to procedural or physical measures. It is not usually practical or cost-effective to add internal controls late in the program. Processing could be restricted to non-sensitive information only or to a lower level of sensitive information than planned. The security mode of operations could also be chanced to provide a higher level of confidence or protection. Selected functions causing major problems or creating high risk could be removed or their implementation delayed. The number of users, or their privileges, could be restricted. Remote terminals could be physically or logically disconnected when sensitive information is stored or processed.

5.2.3 Prepare Accreditation Package

The required information to make an intelligent accreditation decision is contained in the accreditation package. This package presents the Accreditor with a recommendation for an accreditation decision, a statement of residual risk, and supporting documentation which could be a subset of the certification package. It may be in the form of a technical document, technical letter, and/or annotated briefing. Additional documentation from the certification package can be provided to the Accreditor depending on the level of detail they are requesting. Table 5-1 describes the information generally included as part of the accreditation package.

Recommendation for accreditation decision, which includes a residual risk statement and rationale for accepting/rejecting residual risk.

Impact statement attesting, to the criticality of the computer system from the end user or functional area supported.

MOA(s).

Waiver(s), pending, or approved.

System overview including AIS configuration and interconnections (e.g, executive summary from the system security plan).

Site Survey Report (optional).

TABLE 5-1 Accreditation Package

5.3 Activity 7 - Make Accreditation Decision

Activity 7 involves the Accreditor making and documenting the accreditation decision. This decision is based on many factors, such as global threats, certification results/recommendations, residual risks, the availability or cost of alternative countermeasures, operational requirements, and factors that transcend security, such as system need/criticality, program, schedule risks, and political consequences. The Accreditor has a range of options in making the accreditation decision, including the following:

- Full accreditation approval for its originally intended operational environment, including constraints and a recertification/reaccreditation timeline.

- Accreditation for operation outside of the originally intended operational environment (e.g., change in mission, crisis situation, more restrictive operations).

- Interim (temporary) accreditation approval, identifying the tasks to be completed prior to full granting of accreditation and any additional controls (e.g., procedural or physical controls, limiting, the number of users) that must be in place to compensate for any increased risk.

- Accreditation disapproval, including recommendations and timelines for correcting specified deficiencies.

Part of the accreditation decision is the acceptance of a given level of risk against a defined threat with a set of countermeasures. In order to making an informed decision, the Accreditor must be aware of both the definition of threat and the identification of the specific threat as it applies to the system being considered for accreditation. There will always be threats to sensitive information. The threats, coupled with the system's vulnerabilities, provide the risks upon which to focus the security protection features or the countermeasures. The Accreditor must balance (1) the risk of disclosure, loss, or alteration of information, (2) the availability of the system based on the vulnerabilities identified by the certification process, (3) loss of accountability, (4) the threat that these vulnerabilities may be exploited in the specific environment in which the system is being used, (5) the operational need and benefits, (6) the adequacy of the security countermeasures selected, and (7) the cost (e.g, dollars, schedule, performance) to reduce the risks.

In addition, there may be situations where the Accreditor must balance the risk against operational requirements mandating acceptance of higher risk, such as during a crisis situation. While operational needs can dramatically change during a crisis, the need for security is even more critical during these times.

An accreditation decision is in effect after the issuance of a formal, dated statement of accreditation signed by the Accreditor and remains in effect for the specified period of time (varies according to applicable policies). In some cases (e.g., when dealing with new technology during a transition phase, or when additional time is needed for more rigorous testing), the Accreditor may grant an interim approval to operate for a specified period of time. Interim approval allows the activity to meet its operational requirements for a given period of time while further analyzing and improving its security posture. It gives the Accreditor the needed latitude to approve operational implementation of individual components of a system as they develop. The final decision is documented in the Accreditation letter and a sample is included in Appendix L.

SECTION 6

PHASE IV: POST-ACCREDITATION

Various recertification and reaccreditation cycles are currently prescribed. Typically, these range between three and five years. For example, DoD Directive (DODD) 5200.28 and OMB A-130 states that a system shall be reaccredited at least every three years. On the other hand, Director of Central Intelligence (DCI) policy specifies a five year reaccreditation cycle [22]. During this time, periodic reviews of the system should be conducted to ensure that no changes in the system have occurred that might necessitate reaccreditation before the three- or five- year cycle. For systems with multiple Accreditors, recertification and reaccreditation requirements and responsibilities should be identified in the MOA.

6.1 Activity 8 Maintain Accreditation

The Post-Accreditation Phase involves maintaining the system accreditation throughout the system life-cycle. Accreditation maintenance involves ensuring that the system continues to operate within the stated parameters of the accreditation. For example, this phase ensures that the stated procedures and controls of the system (e.g., TFM, SFUG) stay in place and are used, that the environment does not change outside of the stated parameters, that other types of users are not added to the system (e.g., lower cleared users), that no additional external connections are made to the system, or that additional security requirements are not imposed on the system. Any substantial changes to the stated parameters of the accreditation may require that the system be recertified or reaccredited.

It is important to note that recertification and/or reaccreditation activities may differ from those performed in support of a previous accreditation decision. For example, the system security mode of operation may change from system-high to compartmented mode, requiring more stringent security measures and an in-depth analysis of these measures. Applicable security policies/regulations, certification team members, and/or the Accreditor may also change. The certification agreement should form the basis for determining if the system requires recertification.

6.1.2 Review System Modifications

Once a system has been approved to operate, any future modification to the system may invalidate the accreditation. The Accreditor should be involved in the configuration management to the system and have a representative on the CCB. Any requests for a modification to the system should be analyzed for impacts to the security of the system as stated and agreed to in the certification agreement. Some of the modifications that may cause the system to be reaccredited are listed in Appendix H.

6.1.3 Review Vulnerabilities and Threats

Vulnerabilities and threats to a system do not remain static over the life-cycle of the system. Periodically, the Accreditor should review not only the known threats, but remain abreast of any new threats that are identified and determine if the system still adequately protects against these threats. Some of the changes that may cause the system to be recertified are [18]:

- A change in the system mission or CONOPS
- A change in the operating environment
- A change in the technology employed in, or by, this system
- A change in criticality and/or sensitivity level that causes a change in the countermeasures required
- A change in the security policy (e.g., access control policy)
- A change in the system risk (e.g., new threat to which the system is vulnerable)
- A change in the activity that requires a different security mode of operation
- A breach of security, a breach of system integrity, or an unusual situation that appears to invalidate the accreditation by revealing a flaw in security design
- Results of an audit or external assessment
- A new data sensitivity type
- A new group of users with different roles/responsibilities/privileges

Some of the threat changes that may cause the system to be recertified are:

- Adversary acquires new capabilities
- Trusted individual becomes untrusted

- Countermeasure was removed

6.1.4 Repeat Process with Activity 3

When a modification or new threat/vulnerability impacts the certification agreement, the Accreditor should task the CA to recertify the system. If the modification or new threat/ vulnerability causes a change to the certification agreement, the Accreditor, CA, PM, and the user must update and approve a new certification agreement. With an approved certification agreement, the CA should develop a C&A plan for the recertification and reaccreditation of the system. Once the plan is approved, the CA should repeat the process beginning at Activity 3.

APPENDIX A

OTHER C&A DOCUMENTS

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

The DITSCAP defines a standard DoD process to certify and accredit all DoD systems. This document is written to explain the overall process.

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Guidelines

The DITSCAP Application Guidelines provide more detailed guidance to implement the DITSCAP. (To be published).

Introduction to Certification and Accreditation, January 1994, NCSC-TG-029.

This document, which provides an introduction to C&A concepts, provides an introductory discussion of some basic concepts related to C&A and sets the baseline for further documents. Its objectives are the following: (1) to provide an overview of C&A, its function and place within the risk management process; (2) to clarify the critical roles the Accreditor and other key security officials must assume throughout the C&A process; (3)to identify some of the current security policies, emphasizing some key policy issue areas; and (4) to define C&A-related terms.

The Accreditor's Guideline (future)

This document is written for the Accreditor and his/her staff. It is intend to give an understanding of the responsibilities for accrediting an AIS or a network of AISs.

APPENDIX B

C&A ACTIVITIES

Tasks	Input(s)	Output(s)
- Analyze Needs	- System PM - Security policies (e.g., DCID 1/16, DoD-STD-5200.28, OMB Cir A-130) -Responsible Data Item -User clearances -User roles and capabilities - Environmental requirements - System and functional requirements - Operation requirements - External connections - Network connection rules	- Accreditor and other important individuals identities - System specific security policies - Minimum user clearance level - Highest data classification level -Identity of Accreditor for external systems and networks - Accreditation boundary - Network connection rules
- Determine usage requirements that impact C&A	- Accreditation boundary - Security policy - System criticality - Security CONOPS	- High-leveled agreement on C&A effort and security requirements
- Analyze risk-related considerations (initial risk analysis)	- Threat analysis - Initial risk analysis - System capabilities - Minimum user clearance level - Highest data sensitivity level	- System specific risks and threats - Overall risk level or mode of operation - Data sensitivity level
- Determine certification type	- Degrees of assurance (confidentiality, integrity, availability, accountability) - Assurance ranges - Types of certification	- Type of certification - Degrees of assurance for the various categories - Preliminary certification agreement
- Identify C&A team	- Team organization - Team duties and responsibilities - Team training - Reactions with other groups for C&A support	- Certification team - C&A roles and responsibilities - MOUs - Team training - Automated tools - Other support

TABLE B-1
Phase I, Activity 1: Prepare C&A Agreement

Tasks	Input(s)	Output(s)
- Identity secondary factors	- New system acquisition - Follow-on or upgrade to existing system - Existing system - Prototype or COTS integration - System complexity - Security environment	- Life-cycle phase - System milestones (time constraints) - Trustworthiness of development/maintenance
- Determine applicability of documentation	- Contents of certification package (by certification type) - Suggested documentation for each task (by certification type) - Current system documentation - Previous certification or evaluation documentation - Agreement	- Estimate on reusability of evidence - Documentation available - Documentation to produce - Risks created by unavailable documentation - Final Certification Agreement
- Develop C&A plan	- Final Certification Agreement	- C&A Plan

TABLE B-2
Phase I, Activity 2: Plan for C&A

Tasks	Input(s)	Output(s)
- Analyze detailed system information	- C&A Plan - Final Certification Agreement - Facility risk analysis (if facility is complete) - Facility target environment (if facility is not complete) - System security policy - Test documentation - Previous certification evidence - Operational security doctrine	- Analysis results
- Conduct INFOSEC analysis - System security architecture - Life-cycle assurance - Testing - Physical review analysis - Operational security review	- Final Certification Agreement	- Analysis results (e.g., ST&E results) - Task analysis reports - Residual risk -Waivers
- Conduct Vulnerability analysis	- Documentation available - Analysis results - Residual risk	- Alternative countermeasures - Associated costs - Net value - Updated residual risks

TABLE B-3
Phase II, Activity 3: Performing INFOSEC Analysis

Tasks	Input(s)	Output(s)
- Complete certification package	- C&A Plan - Final Certification Agreement - Residual risks - Test results - MOA(S) - Certification letter	- Certification package - Supplemental documentation
- Make accreditation recommendation	- Certification package	- Accreditation recommendations - Caveat/limitations on system operation - Additional security measures

TABLE B-4
Phase II, Activity 4: Report Certification Findings/Recommendations

Tasks	Input(s)	Output(s)
- Conduct site accreditation inspection	- Accreditation package - System configuration - Residual risks - Additional security features	- Updated accreditation recommendation
- Conduct risk analysis	- Final Certification Agreement - Analysis of risk - Residual risk - ST&E results	- Alternative countermeasures - Associated cost - Net value - Usage restrictions - Updated residual risks

TABLE B-5
Phase III, Activity 5: Perform Risk Assessment

Tasks	Input(s)	Output(s)
- Prepare accreditation package	- Accreditation recommendation - Caveats	- Accreditation package
- Make accreditation recommendation	- Certification package	- Accreditation recommendation - Caveats/limitations on system operation - Additional security measures

TABLE B-6
Phase III, Activity 6: prepare Accreditation Recommendation

Tasks	Input(s)	Output(s)
- Determine decision to operate	- Accreditation package - Management considerations - System criticality	- Accreditation decision (written)

TABLE B-7
Phase III, Activity 7: Make Accreditation Decision

Tasks	Input(s)	Output(s)
- Review system modifications	- Engineering Change Proposals (ECPs) - Updated/changes system documentation - CM Plan - Final Certification Agreement	- Requirement for recertification/reaccreditation - Security impacts - Plan for recertification and reaccreditation - Updated and approved certification agreement
- Review vulnerabilities and threats	- Risk analysis - Threat analysis - Residual risk - Contingency plan	- Revised residual risk - Revised contingency plan - Requirement for recertification/reaccreditation - Security impacts -Plan for recertification and reaccreditation - Updated and approved certification agreement
- Repeat process with Activity 3	- See Activity 3	- See Activity 3

TABLE B-8
Phase IV, Activity 8: Maintain Accreditation

APPENDIX C

ADDITIONAL C&A SUPPORT

Title	Responsibility
Operations Manager	Coordinate the systems operation
ISSO	Conduct the risk assessment
Physical Security Officer (fire, police)	Conduct the facility risk assessment
Database Manager	Coordinate database, activities
System Administrator	Coordinate system resources
Facilities Manager	Coordinate the system facilities activities
TEMPEST Officer[1]	Coordinate the TEMPEST activities
COMSEC custodian/account[1]	Coordinate the COMSEC activities

TABLE C-1
Risk Management Team

[1] Only if applicable

Title	Responsibility
Program Manager *	Direct development, operations or maintenance of the system. Define and manage the system schedule and budget. Work with the Accreditor and User Representative to reach agreement on all security critical issues.
Accreditor *	Approve security requirements; review and approve the C&A process tailoring and level-of-effort determination; oversee C&A security evaluations; evaluate threat, vulnerabilities, risk; and make accreditation decision.
User Representative *	Define/validate system performance, availability, and functionality requirements. Support C&A process tailoring, monitor C&A process to ensure accredited system will meet users needs.
Acquisition Organization	Ensure that all roles are carrying out their responsibilities to ensure security issues are being addressed.
Certification Team	Provide guidance, issue resolution, policy adherence, and systems analysis with respect to security.
Integration	Discuss issues on meeting security requirements. Provide input as to how security requirements are being met.
Security Engineering	Ensure that security requirements are being adequately addressed. Provide recommendations on how to meet requirements.
Configuration Management	Ensure that the system security engineering approach is being followed; manage changes to the software, hardware, and documentation.
Maintenance	Provide input to the process and system needs for maintenance, post-IOC**.**
Operations	Discuss issues on operational procedures.
End-User	Provide input as to whether the system being developed will meet the user's needs.
Developer	Discuss issues/problems in meeting the security requirements.
Independent Validation and Verification (TV&V)	Provide unbiased assessment of how and if the system implements the necessary security requirements.
Certification Agent	Responsible for making the technical judgement of system's compliance with stated security requirements. Signs certification package and prepares accreditation package.

Note: * Indicates a principal role and responsibility

TABLE C-2
Information System Security Working Group Membership

APPENDIX D

DATA SENSITIVITY

Data Type	Definition	Examples
National Security Sensitive	Data processed are CONFIDENTIAL, SECRET, TOP SECRET. Process control systems where alteration could result in a catastrophic occurrence.	Stationing systems containing assignments and ship dispositions; drug smuggling tracking systems.
Financial Sensitive (very sensitive)	Data processed are used in direct payment operations. Data compromise or alteration could result in significant legal and financial liability.	Personnel with direct link payroll; electronic funds transfer liability.
Critical Operations (very sensitive)	Alteration or compromise of data contained in or processed by an application could have significant adverse affects on an agency's ability to complete its mission in an effective manner.	Air traffic control systems; weather forecasting.
Personnel (sensitive)	Data stored/processed are covered by the Privacy Act. Data compromise could result in legal liability but not significant financial liability.	Personnel systems without direct link to payroll.
Administrative	Data compromise may cause embarrassment but would not result in legal/financial liability.	Budget planning system.
Proprietary	Information provided by non-Government sources on the condition that it not be released to other non-Government sources.	Company propriety data; contract bids; quality assurance evaluations; pre-award survey information.
Trusted Information	Information that when received is accepted as authentic.	AUTODIN messages; electronic mail messages; digital signatures.
Security Control	Data associated with the security mechanisms.	Passwords; audit records; system configuration data; integrity of the TCB.
Source Selection Sensitive	Information on upcoming contacts and proposals.	Business strategies; Request for Proposal, bids, or information.
Logistics Information	Data concerning the status and allocation of personnel and material to/from various locations.	Unit readiness; weapon status; computing processing capabilities.

TABLE D-1

Data Sensitivity [22.23]

(continued on next page)

Data Type	Definition	Examples
Weapons system acquisition information	Information critical to the development, deployment, and/or life-cycle status of a weapon system and/or support equipment.	Development status; research capabilities/status; delivery schedules; Export Control Act data; funding status.
Nonsensitive	Small programs, easily reconstructed. No effect on agency operations if data are lost or compromised. No financial liability.	Training aids.

TABLE D- 1 (continued)
Data Sensitivity [22,23]

When determining data sensitivity, the term data refers to both mission data (e.g., messages, financial records) and administrative data (e.g., passwords, access control lists).

Data Factors	Weighing Factors		
Percentage of users authorized (e.g., need-to-know and formal access) for all data on the system	<25% (authorized=6)	>=25% and <=99% (authorized=4)	=100% (authorized=0)
Number of Top Secret compartments	>1 (compart=6)	=1 (compart=4)	=0 (compart=0)
Number of different data types from Appendix D, Table D-1	>6 (types=3)	>=4 and <=6 (types=2)	<4 (types=1)
Number of classified categories (e.g., Top Secret, Secret, Confidential)	>1 (class-cat=6)	=1 (class-cat=4)	=0 (class-cat=0)
Percentage of users cleared (but may not have need-to-know) for all data on the system	<25% (cleared=8)	>=25% and <=99% (cleared=6)	=100% (cleared=0)

TABLE D-2
Data Sensitivity Weights

If "compart" equals 0 and "class-cat" equals 0, then data-sensitivity equals "authorized + ((cleared + types) * 2)"

If "compart" or "class-cat" is not equal to 0, data-sensitivity equals "(compart + class-cat) * (authorized + cleared + types)"

APPENDIX E

CERTIFICATION METRICS

Consequences of Loss of Confidentiality	Confidentiality Weighing Factors		
Impact of release of data (data sensitivity from Appendix D, Table D-2)	data sensitivity >59 (w=8)	data sensitivity >=13 and <=59 (w=4)	data sensitivity <13 (w=2)
Loss of life from release of data	very likely (w=10)	not likely (w=5)	n/a (w=0)
Loss of credibility from release of data	very likely (w=5)	likely (w=3)	n/a (w=0)
Financial loss from release of data	>20% of operating budget per incident (w=5)	>=5% and <=20% of operating budget per incident (w=3)	<5% of operating budget per incident (w=1) n/a (w=0)
Civil penalties/fines for release of data	>=$10,00 per incident (w=5)	<$10,000 per incident (w=3)	n/a (w=0)

TABLE E-1 Confidentiality Metric

Consequences of Loss of Integrity	Integrity Weighing Factors		
Loss of credibility from integrity failure (system or data)	very likely (w=5)	likely (w=3)	n/a (w=0)
Loss of life from integrity failure (system or data)	very likely (w=10)	likely (w=5)	n/a (w=0)
Civil penalties/fines for integrity failure	>=$10,000 per incident (w=5)	<$10,000 per incident (w=3)	n/a (w=0)
Financial loss from integrity failure	>20% of operating budget per incident (w=5)	>=5% and <=20% of operating budget per incident (w=3)	<5% of operating budget per incident (w=1) n/a (w=0)

Consequences of Loss of Availability	Availability Weighing Factors		
Loss of credibility from system failure	very likely (w=5)	likely (w=3)	n/a (w=0)
Loss of life from system failure	very likely (w=10)	likely (w=5)	n/a (w=0)
Financial loss from system failure	>20%of operating budget per incident (w=5)	>=5% and <=20% of operating budget per incident (w=3)	<5% of operating budget per incident (w=1) n/a (w=0)
Disruption of critical service [1]	very likely (w=4)	likely (w=3)	n/a (w=0)
Civil penalties/ fines for loss of availability	>=$10,000 per incident (w=5)	<$10,000 per incident (w=3)	n/a (w=0)

[1] Disruption of service is defined as a resource not being available within a predetermined time.

Consequences of Loss of Accountability	Accountability Weighing Factors		
Civil penalties/fines for loss of accountability	>=$ 10,000 per incident (w=5)	<$10,000 per incident (w=3)	n/a (w=0)
Loss of from accountability failure	very likely (w=10)	likely (w=5)	n/a (w=0)
Loss of credibility from accountability failure	very likely (w=5)	likely (w=3)	n/a (w=0)
Financial loss from accountability failure	>20% of operating budget per incident (w=5)	>=5% and <=20% of operating budget per incident (w=3)	<5% of operating budget per incident (w=1) n/a (w=0)

TABLE E-4 Accountability Metric

Personnel Authorization Requirements	Y	N	N/A
Are factory installed accounts, privileges, and passwords deleted when the system is installed?			
Is authentication (e.g., passwords) unique to an individual?			
Is each user's authentication changed on a periodic basis as required by the Security Policy?			
Is each user's authentication randomly generated?			
If passwords are used, are they at least 6 characters in length?			
Is each user's authentication electronically distributed?			
Has a procedure been established for requesting an authentication?			
Is user access removed when no longer needed?			
Is preventive maintenance performed at the prescribed intervals?			
Are individuals only given the minimum capabilities required to perform their assigned duties?			

TABLE F-2 Personnel Authorization Checklist

Risk Management Requirements	Y	N	N/A
Has a contingency plan been developed?			
Has the contingency plan been successfully tested in the past year?			
Is the contingency plan periodically reviewed and updated?			
Does the contingency plan address fire, flood, civil disorder, natural disaster, and bomb threat?			
Is emergency lighting installed and is it periodically tested?			
Is the system free of overhead steam or water pipes (other for fire suppression)?			
Do backups occur routinely for essential user data?			
Is the backup data protected from destruction and/or tampering?			
Are backup procedures in place and tested to conduct essential system tasks after a disruption to the primary facility/system?			
Are recovery procedures in place and tested to permit rapid restoration of the system following a disruption to the primary facility/system?			
Has an alternate site been identified with compatible equipment?			
Has the alternate site been tested during the past year?			
Is at least a surge protector installed for each piece of hardware? Are emergency exits clearly marked?			
Has a risk analysis of the system been completed in the past three years?			
Has the ISSO developed security incident response procedures?			

TABLE F-3 Risk Management Checklist [24]

Personnel Security Requirements	Y	N	N/A
Do all personnel gaining access to the system have a need-to-know?			
Are escort procedures established for all visitors (e.g., maintenance personnel)?			
Is access to the system canceled when individuals leave the organization or no longer need access?			

TABLE F-4 Personnel Security Checklist [24]

Network Requirements	Y	N	N/A
Has a Network Security Officer (NSO) been appointed?			
Are the duties and responsibilities of the NSO defined in writing?			
Does this system, or network, comply with the connection rules for the system(s) or networks to which it is attached?			
Has a security policy n established for this system?			
Is that security policy enforced in the connection to other systems and accesses available from external users and processes?			
Does the NS0 maintain a liaison with the other ISSOs/NSOs on the network?			

TABLE F-5 Network Security Checklist [24]

ST&E Requirements	Y	N	N/A
Has an ST&E been conducted and the results fully documented?			
Does the ISSO ensure an ST&E is performed on all system upgrades?			
Is the ISSO involved in developing/reviewing test plans for installation of system upgrades?			

TABLE F-6 ST&E Checklist [24]

Classified System Requirements	Y	N	N/A
Has a TEMPEST survey been completed and TEMPEST zones established?			
Has a TEMPEST Officer been appointed?			
Has a TEMPEST countermeasure evaluation been completed?			
Is the TEMPEST Officer involved in all hardware installations?			
Does the TEMPEST Officer approve all equipment moves?			
If COMSEC is included:			
a)Has a COMSEC custodian been appointed?			
b)Has a key management program been established?			
c)Has a COMSEC accountant been appointed?			
Have procedures been established for declassifying the system?			
Are all products produced by the system (e.g., listings, tapes, disks) marked with the highest classification of the system?			
Have procedures been established for destruction/safeguarding of classified if the facility must be evacuated?			
If Top Secret (TS)/Sensitive Compartmented Information (SCI) is processed, has a SCIF been approved?			

TABLE F-7 Classified System Checklist [24]

Configuration Management Requirements	Y	N	N/A
Is an inventory kept of the hardware, software, firmware, and documentation?			
Has the ISSO developed and implemented procedures to inspect software for malicious code prior to its installation?			
Is the ISSO informed of changes to the system prior to their installation?			
Has the ISSO developed and implemented procedures to keep unauthorized hardware, software, and firmware off of the system?			
Have procedures been implemented to ensure the correct version of hardware, software, firmware, and documentation are installed/ available?			
Has the ISSO developed procedures to search for and remove malicious code from the system?			
Is a backup copy of the applications software, operating system, and system utilities maintained and protected from destruction and/ or tampering?			

TABLE F-8 Configuration Management Checklist [24]

Training Requirements	Y	N	N/A
Does the ISSO have the proper training?			
Does the ISSO provide initial security training to newly assigned personnel?			
Does The ISSO provide periodic security training to all system users?			
Does the user know to report potential security violations to the ISSO?			
Do all system operators receive periodic training on system shut down/start up operation of emergency power and operation of fire and alarm systems?			

TABLE F-9 Training Checklist [24]

Media Handling Requirements	Y	N	N/A
Have procedures been established for the proper disposal/ destruction of system products (e.g., disks, tapes, microfilm)?			
Have procedures been established to ensure distribution of system products (e.g. listings, disks, tapes. microfilm) only to authorize users?			
Is all system generated output carry marked at the top and bottom of each page?			
Are all magnetic storage devices clearly labeled with the highest category of data they contain?			

TABLE F-10 Media Handling Checklist

Physical Security Requirements	Y	N	N/A
During operational hours is the critical computer facility manned by at least two authorized personnel?			
Is an access roster maintained at each entry point to the central computer facility?			
Are all terminal areas physically secured at the end of the day?			
Are positive personnel identification measures (e.g., badge system, finger prints) in place?			
Are visitors to the facility easy to identify (e.g., special badge)?			

TABLE F-11 Physical Security Checklist

APPENDIX G

CERTIFICATION AGREEMENT

The Certification Agreement is a living document that represents the formal agreement among the DAA, User Representative, and the Program Manager. The Certification Agreement is developed in Activity 1 and updated in each phase as the system development progresses and new information becomes available. At minimum, the Certification Agreement will contain the information in the following sample format:

SECTION 1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

1.1 System name and identification
1.2 System mission
1.3 System description
- Functional description
- System capabilities
- System criticality
- Classification and sensitivity of data processed
- System user description and clearance levels
- Life-cycle of the system

1.4 System Concept of Operations summary

SECTION 2. ENVIRONMENT DESCRIPTION

2.1 Operating environment
2.2 Software development and maintenance environment
2.3 Threat description

SECTION 3. SYSTEM ARCHITECTURAL DESCRIPTION

3.1 Hardware
3.2 Software
3.3 Firmware
3.4 System interfaces and external connections
3.5 Data flow (including data flow diagrams)
3.6 TAFIM[1] Security View

[1] Department of Defense Technical Architecture Framework for Information Management (TAFIM), Volume 6, DoD

3.7 Accreditation boundary

SECTION 4. SYSTEM SECURITY REQUIREMENTS

4.1 National/DoD Security Requirements
4.2 Governing Security Requisites
4.3 Data Security Requirements
4.4 Security Concept of Operations
4.5 Security Policy
4.6 Network Connection Rules
- To connect to this system
- To connect to the other systems defined in the CONOPS

4.7 Configuration and Change Management Requirements
4.8 Reaccreditation Requirements

SECTION 5. ORGANIZATIONS AND RESOURCES

5.1 Identification of Organizations
- DAA
- CA
- Identification of the User Representative
- Identification of the organization responsible for the system
- Identification of the Program Manager or System Manager

5.2 Resources
- Staffing requirements.
- Funding requirements

5.3 Training for certification team
5.4 Roles and responsibilities
5.5 Other supporting organizations or working groups
5.6 Roles and responsibilities

SECTION 6. CERTIFICATION PLAN

6.1 Tailoring factors
- Programmatic considerations
- Security environment
- System characteristics
- Reuse of previously approved solutions Tailoring summary

6.2 Tasks and Milestones
6.3 Schedule summary
6.4 Level of effort
6.5 Roles and responsibilities

APPENDICES: SYSTEM CERTIFICATION AND ACCREDITATION ARTIFACTS

(Include all documentation that will be relevant to the systems C&A.)

APPENDIX	A	Acronym List
APPENDIX	B	Glossary of Terms
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	Certifiers Recommendation
APPENDIX	I	Contingency Plan(s)
APPENDIX	J	Security Awareness and Training Plan
APPENDIX	K	Incident Response Plan
APPENDIX	L	Memorandums of Agreement
APPENDIX	M	Applicable System Development Artifacts or System Documentation
APPENDIX	N	Accreditation Documentation and Accreditation Statement

Other Appendices may be added as needed. Examples include

- C&A Work Plan and Project Charts
- ST&E Results and Test Report
- Vulnerability Assessment and Statement of Residual Risk
- Security Operating Procedures

APPENDIX H

UPGRADES TO EXISTING SYSTEMS

Upgrade/change in operating system

Change in database management system

Upgrade to Central Processing Unit (CPU)

Upgrade to device drivers

A change to the TCB as specified in the Security Policy

A change to the applications software as specified in the Security Policy

A change in criticality and/or sensitivity level that causes a change in the countermeasures required

A change in the security policy (e.g., access control policy)

Additions or a change to the hardware that requires a change in the approved security countermeasures

A significant change to the configuration of the system (e.g., a workstation is connected to the system outside of the approved configuration)

Connection to a network

For networks**,** the inclusion of an additional (separately accredited) system(s) or the modification/replacement of a subscribing system that affects the security of system

Introduction of new countermeasures technology

TABLE H-1 Reasons for Recertification

APPENDIX I

CERTIFICATION PACKAGES

1. Certification Letter (signed by the CA; for larger systems)

2. Residual risk statement including rationale for why residual risks should

3. Certification Agreement

4. MOAs/MOUs with interconnected systems

5. Waivers Pending or Approved (Waivers should always be subject to periodic review. The risks to be accepted by virtue of the waiver should be clearly identified

6. Assurance rationale (tables from Appendix E)

7. Security Policy

8. C&A Plan

9. INFOSEC countermures Cost/Benefit Analysis

10. Operational Test and Evaluation (OT&E) Test Reports (or security-relevant extract if security testing was incorporated in other tests and not done separately)

11. Statements from the responsible Government agencies indicating that personnel, physical, COMSEC, or other security requirements have been met (e.g., Defense Message System (DMS) Connection Approval Process (CAP) functional testing)

TABLE I-1
Type 2 Certification Package [13]

1. SFUG

2. TFM

3. Developmental Test and Evaluation (DT&E) Test Plans (or security-relevant extract)

4. OT&E Test Plans (or Security-relevant extract)

5. Contingency plan

6. CM Plan, EPL FER (unclassified)

7. Summary Reports for each task defined for Type 2

TABLE I-2
Type 2 Supplemental Documentation [13]

1. Certification Letter (signed by the CA for larger systems)

2. Residual risk statement including rationale for why residual risks should be accepted/rejected

3. Certification Agreement

4. MOAs with interconnected systems

5. Waivers Pending or Approved (Waivers should always be subject to periodic review. The risks to be accepted by virtue of the waiver should be clearly identified.)

6. Assurance rationale (tables from Appendix E)

7. Security Policy

8. C&A Plan

9. INFOSEC countermeasures Cost/Benefit Analysis

10. DT&E or OT&E T Reports (or security-relevant extract if security testing was incorporated in other tests and not done separately)

11. Statements from the responsible Government agencies indicating that personnel, physical, COMSEC, or other security requirements have been met (e.g., DMS CAP function testing)

12. Other Pertinent Documents (e.g., IV&V Reports)

TABLE I-3
Type 2 Certification Package [13]

1. SFUG

2. TFM

3. DT&E Test Plan (or security-relevant extract)

4. OT&E Test Plans (or security-relevant extract)

5. System Security CONOPS

6. System security architecture

7. Executive Summary from the DTLS and the FILS

8. Evaluation of the use of security features (e.g., TCB) found in the hardware and software of an system.

9. CM Plan, EPL FER (unclassified), Security Classification Guide, Site Surveys, other agencies not directly part of the certification team.

10. Contingency plan

11. Reports for each task defined for Type 3

TABLE I-4
Type 3 Supplemental Documentation [13]

1. Certification Letter (signed by the CA; for larger systems)
2. Residual risk statement, including rationale for why residual risks should be accepted/rejected
3. Certification Agreement
4. MOAs/MOUs with interconnected systems
5. Waivers Pending or Approved (Waivers should always be subject to periodic review. The risks to be accepted by virtue of the waiver should be clearly identified.)
6. Assurance rationale (tables from Appendix E)
7. Security Policy
8. C&A Plan
9. INFOSEC countermeasures Cost/Benefit Analysis
10. DT&E or OT&E Test Reports (or security-relevant extract if security testing was incorporated in other tests and not done separately)
11. Statements from the responsible Government agencies indicating that personnel, physical, COMSEC, or other security requirements have been met (e.g., DMS CAP functional testing)
12. Other Pertinent Documents (e.g., IV&V Reports)

TABLE I-5
Type 4 Certification Package [13]

1. SFUG

2. TFM

3. DT&E Test Plans (or security-relevant extract)

4. OT&E Test Plans (or security-relevant extract)

5. System Security CONOPS

6. System security architecture

7. Executive Summary from the Descriptive Top-Level Specification and the Formal Top-Level Specification

8. Covert Channel Analysis Report

9. Evaluation of the use of security features (e.g., TCB) found in the hardware and software of an system.

10. CM Plan, EPL FER (unclassified), Security Classification Guide, Site Surveys, other agencies not directly part of the certification team.

11. Continency plan

12. Summary Reports for each task defined for Type 4

TABLE I-6
Type 4 Supplemental Documentation [13]

APPENDIX J

SUMMARY REPORT FORMAT

Task performed (e.g., Task 1 - System Architecture Study)

Level of Effort (2, or 3, or 4)

Documentation available:

Documentation not available:

Documentation used:

References used:

Names and organizations of individual(s) performing task:

Resources needed (e.g., system time, test equipment, test tools, CASE tools):

Time needed to complete task:

Problems encountered in completing task (e.g., lack of time, team training):

System strong points:

System weaknesses:

Suggested system improvements (e.g., countermeasures):

Implemented system improvements:

Suggestions to improve suitability of task to aid in the analysis of the system:

APPENDIX K

SAMPLE CERTIFICATION LETTER

To: [Accreditor(s)]

From: [Certification Agent]

Subj: System Security Certification of (name of system activity]

Ref: (a) [name of implementing regulation]
(b) [letter from activity requesting certification]
(c) Certification support documentation

Encl: (1) List of system elements for which recreation is being requested
(2) Overall degree of assurance for the system (to include the degrees of assurance for
(3) Residual risk(s) of operating the system
(4) Draft Accreditation Letter

1. In accordance with the provisions of reference (a) and as requested by reference (b), the certification team under my direction has reviewed and analyzed the implementation of the security requirements of the system identified in enclosure 1. The degree of assurance required by the users of the system is listed in enclosure 2 and was the driving force in determining the level of effort needed for the certification of this system. Our analysis identified [X] residual risk(s) of operating this system in the specific environment. These residual risks are listed in enclosure 3.

2. Due to the residual risks of operating the system, I recommend the system [be granted full accreditation, be granted interim accreditation, be disapproved for accreditation and you sign the Accreditation letter in enclosure [4].

3. A copy of this certification letter with supporting documentation will be retained by the activity as a permanent record.

[Certification Agent's signature block]

APPENDIX L

SAMPLE ACCREDITATION LETTERS [18]

GRANT FULL ACCREDITATION

To: [Senior Official of system activity]

From: [Accreditor(s)]

Subj: SYSTEM SECURITY ACCREDITATION OF [name of system activity]
Ref: (a) [name of implementing regulation]
(b) [letter from activity requesting accreditation]
(c) Accreditation support documentation

Encl: (1) List of system elements for which accreditation is being granted
(2) List of system elements which are directed to e operation

1. In accordance with the provisions of reference (a) and as requested by reference (b), I hereby grant full accreditation to [name of system activity and location]. This accreditation is based upon a review of the information provided in reference (c). This accreditation is my formal declaration that appropriate system security countermeasures have been properly implemented and that a satisfactory level of security is present. Enclosure (1) identifies the individual system elements of the activity and the classification of data each is authorized to process the security mode of operation and any special conditions that apply. [Tailor this last sentence as needed to include any caveats to the type of Approval to Operate.) Enclosure (2) identifies the system components that will cease operation and the projected date of this action.

2. This accreditation is valid for [X] years from the date of letter [depends on the Accreditor(s) and any caveats listed in paragraph 1]. Reaccreditation is required sooner if there is a change affecting the system security posture of the activity. It is the responsibility of the senior official in charge of the system to ensure that any change in configuration mode of operation or other modification is analyzed to determine its impact on system security and that appropriate action is taken to maintain a level of security consistent with the requirements for this action.

3. A copy of s accreditation letter with supporting documentation will be retained by the activity as a permanent record.

[Accreditor(s) signature block]
GRANT INTERIM ACCREDITATION

To: [Senior Official of system activity]

From: [Accreditor(s)]

Subj: SYSTEM SECURITY ACCREDITATION OF [name of system activity]

Ref: (a) [name of implementing regulation]
(b) [letter from activity requesting accreditation]
(c) Accreditation support documentation

Encl: (1) List of system elements assigned an interim authority to operate
(2) List of additional system security countermeasures required for full accreditation
(3) List of system elements which are directed to cease operation

1. In accordance with the provisions of reference (a) and as requested by reference (b), I hereby grant interim accreditation to [name of system activity and location]. This accreditation is based upon a review of the information provided in reference (c). This accreditation is my formal declaration that some system security countermures have been properly implemented; however, additional system security countermeasures are needed to ensure that a satisfactory level of security is present. Enclosure (1) identifies the individual system elements of the activity and the classification of data each is authorized to process, the security mode of operation, and any special conditions that apply. Enclosure (2) identifies additional system security measures that must be implemented in order to achieve full accreditation. [Tailor the previous sentence as needed to include any caveats to the type of Approval to Operate. Interim approval to operate may be used to allow a system to begin testing in its operational environment, but some caveats may still be warranted.) Enclosure (3) identifies the system components that will cease operation and the projected date of this action.

2. This interim accreditation is valid for [X period of time] from the date of this letter [depends on the Accreditor(s) and any caveats listed in paragraph 1]. Reaccreditation is required sooner if there is a change affecting the system security posture of the activity. It is the responsibility of the senior official in charge of the system to ensure that any change in configuration, mode of operation, or other modification is analyzed to determine its impact on system security and that appropriate action is taken to maintain a level of security consistent with the requirements for this accreditation.

3. A copy of this accreditation letter with supporting documentation be retained by the activity as a permanent record

[Accreditor(s)'s signature block]

DISAPPROVE ACCREDITATION

To: [Senior Official of system activity]

From: [Accreditor(s)]

Subj: SYSTFM SECURITY ACCREDITATION OF [name of system activity

Ref: (a) [name of implementing regulation]
(b) Better from activity requesting accreditation]

Encl: (1) List of system elements not approved to operate
(2) List of additional system security countermeasures required for accreditation
(3) List of system elements which are directed to cease operation

1. In accordance with the provisions of reference (a) and as requested reference (b), hereby disapprove accreditation to (name of system activity and location]. This disapproval is based upon a review of the information provided in reference (c). This disapproval is my formal declaration that inadequate system security countermeasures have been implemented and additional system security countermures are needed ensure that a satisfactory level of security is present. Enclosure (1) identifies the individual system elements of the activity that are disapproved to operate. Enclose (2) identifies additional system security measures that must be implemented in order achieve full accreditation. Enclosure (3) identifies the system components that will cease operation and the projected date of this action.

2. It is the responsibility of the senior official in charge of the system to ensure that system is not operational and the additional countermeasures listed in enclosure (2) are properly implemented. The senior official will also ensure that the Certification Team analyzes the implementation of the additional countermeasures and submits a new certification letter prior to the system becoming operational.

3. A copy of disapproval letter with supporting documentation be retained by the activity as a permanent record.

[Accreditor(s)■s signature block]

LIST OF REFERENCES

1. National Computer Security Center, Introduction to Certification and Accreditation (NCSC-TG-029), January 1994.

2. National Security Telecommunications and Information Systems Security Committee National Information Systems Security (INFOSEC) Glossary (NSTISSI No. 4009), 5 June 1992.

3. INFOSEC Management Panel Committee Working Group (IMP CWG) Report, A Proposed DOD Certification and Accreditation Standard (IW CWG Publication 92- 1, Version 1.0), 16 October 1992.

4. Report Security System Engineering: Composite Analysis Report, Volume 2 - Architect's Handbook (draft) xxxxx), 6 October 1993.

5. DoD Computer Security Center, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (CSC-STD-00385), 25 June 1985.

6. DoD, Information Technology Security Certification and Accreditation Process (DITSCAP) (draft), 30 November 1995.

7. Air Force Regulation (AFR) 205-16, Computer Security Policy, April 1989.

8. NASA Handbook 2410.9, NASA Automated Information Security Handbook, September 1990.

9. U.S. Department of Energy (DOE): Risk Assessment Methodology (NISTIR 4325, reprints DOE-365, September 1989), May 1990.

10. National Institute of Standards and Technology/U.S. Department of Health and Human Services: U.S. Department of Health and Human Services Automated Information Systems Security Program Handbook (NISTIR 4635), July 1991.

11. Office of the Auditor General of Canada: Information Sensitivity and Security

Assessment for Computer Information Holdings.

12. National Institute of Standards and Technology, Guideline for Automated Data Processing Risk Analysis (FIPS PUB 65), August 1985.

13. National Computer Security Center, A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements (NCSC-TG024, Version 1), December 1992.

14. Arca Systems, Inc. Guidance for Developing a Certification and Accreditation Plan (draft), 28 April 1993.
15. Information Systems Security Organization, Information System Security Policy Guideline (draft), 1 April 1993.

16. DoD Computer Security Center, Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (CSC-STD-003-85), 25 June 1985.

17. MITRE Report, Guidelines for Certification of Existing Sensitive Systems (MTR-WI8), July 1982.

18. Information Systems Security Organization, DAA Handbook (draft) (CA-003), 10 April 1993.

19. Dr. Dixie Baker, Dr. Deborah Downs, Frank Belvin, Dr. Santosh Chokhani, James L. Arnold Jr., and Ronald J. Bottomly, Trusted Computer System Architecture: Assessing Modularity, 18 December 1992.

20. Office of Security Information Systems Group, Elements of Secure Computing, August 1992.

21. National Computer Security Center, Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD), December 1985.

22. U.S. General Services Administration, Office of Technical Assistance: Information Technology Installation S

23. Defense Logistics Agency (DLA) Regulation No. 5200.17, 9 October 1991.

24. Department of the Navy, Automated Information Systems Security Guidelines.

25. Management of Federal Information Resouce (OMB Circular A-130), Feb. 8, 1996.

26. Management Accountability and Control (OMB Circular A-123), 21 June 1995.

27. Financial Management Systems (OMB Circular A-127), 23 July 1993.

ACRONYMS

AIS	automated information system
AFR	Air Force Regulation
CA	certification authority
C&A	certification and accreditation
CAP	connection approval process
CCB	Configuration Control Board
CI	configuration item
CM	configuration management
COMPUSEC	computer security
COMSEC	communications security
CONOPS	concept of operations
COTS	commercial-off-the-shelf
CPU	central processing unit
CTTA	Certified TEMPEST Technical Authority
DAC	discretionary access control
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DITSCAP	DoD Information Technology Security Certification and Accreditation
DLA	Defense Logistics Agency
DMS	Defense Message System
DOE	Department of Energy
DoD	Department of Defense
DODD	Department of Defense Directive
DT&E	development test & evaluation
DTLS	Descriptive top-level specification
ECP	engineering change proposal
EPL	evaluated products list
FCA	functional configuration audit
FER	final evaluation report
FIPS	federal Information Processing Standard
FSRS	functional security requirements specification
FTLS	formal top-level specification
GOTS	Government-off-the-shelf

HVAC	heating/ventilation/air conditioning
I&A	Identification and authentication
INFOSEC	information systems security
I/O	input/output
IOC	initial operational capability
ISSO	information systems security officer
ISSWG	information systems security working group
IV&V	independent validation and verification
LAN	local area network
MAC	mandatory access control
MOA	memorandum of agreement
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSO	network security officer
OI	operating instruction
OMB	Office of Management and Budget
OPSEC	operations security
OT&E	operational test and evaluation
PC	personal computer
PCA	physical configuration audit
PM	program manager
RFP	request for proposal
ROM	rough order of magnitude
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SFUG	security features user's guide
SOW	statement of work
ST&E	security test and evaluation
TASO	terminal area security officer
TCB	trusted computing base
TFM	trusted computing base
TRANSEC	transmission security

TS	top secret
WAN	wide area network

GLOSSARY

Accountability

The property that allows the ability to identify, verify, and trace system entities as well as changes in status. Accountability is considered to include authenticity and nonrepudiation.

Accreditation

The formal declaration by an Accreditor that an automated information system (AIS) is approved to operate in a particular security mode using a prescribed set of safeguards Ill.

Accreditor

The term Accreditor will be used synonymously with Designated Approving Authority. See Designated Approving Authority.

Assurance

A measure of confidence that the security features and architecture of an AIS accurately mate and enforce the security policy [1] and is composed of the degree of availability, confidentiality, accountability, and integrity required of the system.

Authentication

Security services designed to establish the variety of a transmission, message, or originator, or a means of verifying, an individual's eligibility to receive specific categories of information [2].

Authenticity

The property that system events are initiated by and traceable to authorized entities.

Availability

The property of being accessible and usable upon demand by an authorized user [1].

Certification

The comprehensive assessment of the technical and nontechnical security features and other safeguards of a system to establish the extent to which a particular system meets a set of specified security requirements for its use and environment [1].

Confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, or processed [l].

Data Integrity

The attribute of data relating to the preservation of (1) its meaning, and completeness; (2) the consistency of its representations; and (3) its correspondence to what it represents [1].

Designated Approving Authority "(DAA - Accreditor)"

Official with authority to formally assume responsibility for operating an AIS or network at an acceptable level of risk. [2]

Integrity

The property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

Nonrepudiation

Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity so that neither can later deny having processed the data [2].

Security CONOPS

A high-level description of how the security of the system operates and a general description of the security characteristics of the system, such as user clearances, data sensitivity, and data flows [1]. Refer to [15] for guidance on developing a system security policy.

Security Policy

The set of laws, rules, and practices that regulate how sensitive or critical information is managed , protected, and distributed [1].

System Integrity

The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system [1].

Threat

The capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or an information system [2].

Type accreditation

The official authorization by the Accreditor to employ a system in a specified environment. It includes a statement of residual risk, delineates the operating environment, and identifies specific use, operational constraints, and/or procedural work around. It may be performed when multiple platforms will be fielded in similar environments [1].

Index

PUBLICATION INFORMATION

Single copies of this document may be obtained by contacting:

DIRECTOR
National Security Agency
INFOSEC Awareness Division
ATTN: Y13/IAOC

Fort George G. Meade, MD 20755-60

For comments or suggestions on this document, write to:

DISA/CISS
701 S. Courthouse Drive
Arlington, VA 22041-3230
Attn. Center for Information Systems Security