DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP)

APPLICATION MANUAL

July 31, 2000

Assistant Secretary of Defense for
Command, Control, Communications,
and Intelligence

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

July 31, 2000

FOREWORD

This Manual is issued under the authority of DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997. It provides implementation guidance to standardize the certification and accreditation process throughout DoD.

This Manual applies to the Office of the Secretary of Defense (OSD), Military Departments, the Chairman of the Joint Chiefs of Staff, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components"). This Manual is effective immediately; it is mandatory for use by all DoD Components.

Send recommended changes to this Manual to:

Defense Information Systems Agency
Information Assurance Program Management Office (D25)
5113 Leesburg Pike, Suite 400
Falls Church, VA 22041

The DoD Components may obtain copies of this Manual through their own publication channels. Approved for public release; distribution unlimited. Authorized registered users may obtain copies of this Manual from the Defense Technical Information Center, Cameron Station, Alexandria, VA 22304-6145. Other Federal Agencies and the public may obtain copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161. This publication is also available at http:\\web7.whs.osd.mil.

Arthur L. Money
Assistant Secretary of Defense
Command, Control, Communications and Intelligence

TABLE OF CONTENTS

REFERENCES

(a) Office of Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) Memorandum, "The Defense Information Systems Security Program (DISSP)," August 19, 1992

(b) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

(c) Public Law 100-235, "Computer Security Act of 1987," January 8, 1998

(d) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources, " February 8 , 1996

(e) Director of Central Intelligence Directive (DCID) 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks," March 14, 1988, replaced by DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 5, 1999

(f) DoD Directive 5220.22, "Industrial Security Program," December 8, 1980

(g) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997

(h) DoD Directive 5000.1, "Defense Acquisition," March 15, 1996

(i) DoD 5000.2-R, "Mandatory Procedures for Major Defense Programs (MDAPS) and Major Automated Information Systems (MAIS) Acquisition Programs," March 15, 1996

(j) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, "National Information Systems Security (INFOSEC) Glossary," January 1999

(k) National Institute of Standards and Technology (NIST) Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," October 1995

(l) Office of Management and Budget Circular No. A-123, "Management Accountability and Control," June 21, 1995

(m) DoD 5200.28-STD, "DoD Trusted Computer Security Evaluation Criteria," December 1985

(n) Defense Systems Management College, "Systems Engineering Management Guide," January 1990

(o) NIST Special Publication 800-4, "Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials," March 1992

(p) NCSC-TG-012, "Trusted Database Management System Interpretation," April 1991

(q) NCSC-TG-028, "Assessing Controlled Access Protection," May 25, 1992

(r) NCSC-TG-021, Version 1, "A Guide to Understanding Design Documentation in Trusted Systems," October 2, 1988

(s) NCSC-TG-011, Version 1, "Trusted Network Interpretation Environments Guideline," August 1, 1990

(t) NCSC-TG-022, "A Guide to Understanding Trusted Recovery in Trusted Systems," December 30, 1991

(u) FIPS Publication 101, "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software," June 6, 1983

(v) NIST Special Publication 500-165, "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards," September 1989

(w) NIST Special Publication 800-6, "Automated Tools for Testing Computer System Vulnerability," December 1992

(x) NCSC-TG-001, Version 2, "A Guide to Understanding Audit in Trusted Systems," June 1, 1988

(y) NCSC-TG-003, Version 1, "A Guide to Understanding Discretionary Access Control in Trusted Systems," September 30, 1987

(z) NCSC-TG-017, Version 1, "A Guide to Understanding Identification and Authentication in Trusted Systems," September 1991

(aa) NCSC-TG-018, Version 1, "A Guide to Understanding Object Reuse in Trusted Systems," July 1, 1991

(ab) MIL-STD-973, "Configuration Management Military Standard," April 17, 1992

(ac) NCSC-TG-006, Version 1, "A Guide to Understanding Configuration Management in Trusted Systems," March 28, 1988

(ad) NCSC-TG-008, Version 1, "A Guide to Understanding Trusted Distribution in Trusted Systems," December 18, 1988

(ae) NCSC-TG-013, "Rating Maintenance Phase Program Documentation"

(af) NCSC-TG-015, Version 1, "A Guide to Understanding Trusted Facility Management," October 18, 1989

(ag) FIPS Publication 31, "Guidelines for Automatic Data Processing Physical and Risk Management," June 1974

(ah) FIPS Publication 65, "Guideline for Automatic Data Processing Risk Analysis," August 1, 1993

(ai) NSTISSAM TEMPEST/1-92, "Compromising Emanations Laboratory Test Requirements, Electromagnetics," December 15, 1992

(aj) NSTISSAM TEMPEST/1-93, "Compromising Emanations Field Test Requirements, Electromagnetics," August 30, 1993

(ak) NSTISSAM TEMPEST/2-92, "Procedures for TEMPEST Zoning," December 30, 1992

(al) NACSIM 5203, "Guidelines for Facility Design and RED/BLACK Installation," June 1, 1982

(am) DoD Directive C-5200.5, "Communications Security (COMSEC)," October 6, 1981

(an) DoD C-5030.58-M, "Defense Special Security Communications: Security Criteria and Telecommunications Guidance," July 1978

(ao) NTISSD 600, "Communications Security (COMSEC) Monitoring," April 10, 1990

(ap) NSA DS-80, "INFOSEC Software Engineering Standards and Practices Manual," January 9, 1991

(aq) FIPS Publication 112, "Password Usage," May 30, 1985

(ar) FIPS Publication 113, "Computer Data Authentication," May 30, 1985

(as) FIPS Publication 87, "Guidelines for ADP Contingency Planning," March 27, 1981

(at) Subchapter 552a of title 5, United States Code

(au) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998

(av) Office of Management and Budget Circular No. A-109, "Major Systems Acquisition," April 5, 1976

DL1. DEFINITIONS

The terms used in this publication were selected from the NSTISSI 4009 (reference (j)) definitions when possible. Where new terms are used, the revised or new definitions will be submitted as changes to reference (j).

DL1.1.1. Accountability. Property that allows auditing of IS activities to be traced to persons or processes that may then be held responsible for their actions. Accountability includes authenticity and non-repudiation.

DL1.1.2. Accreditation. Formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

DL1.1.3. Acquisition Organization. The Government organization that is responsible for developing a system.

DL1.1.4. Active System. A system connected directly to one or more other systems. Active systems are physically connected and have a logical relationship to other systems.

DL1.1.5. Architecture. The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment, and services, including support services and related resources.

DL1.1.6. Assurance. Measure of confidence that the security features, practices, procedures and architecture of an IS accurately mediates and enforces the security policy.

DL1.1.7. Authenticity. Property that allows the ability to validate the claimed identity of a system entity.

DL1.1.8. Availability. Timely, reliable access to data and information services for authorized users.

DL1.1.9. Audit. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established

policies and operational procedures, and to recommend changes in controls, policies, or procedures.

DL1.1.10. Benign System. A system that is not related to any other system. Benign systems are closed communities without physical connection or logical relationship to any other system. Benign systems are operated exclusive of one another and do not share users, information, or end processing with other systems.

DL1.1.11. Certification. Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

DL1.1.12. Certification Authority (Certifier). Individual responsible for making a technical judgement of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation package.

DL1.1.13. Certification Requirements Review (CRR). The review conducted by the DAA, Certifier, program manager, and user representative to review and approve all information contained in the System Security Authorization Agreement (SSAA). The CRR is conducted before the end of Phase 1.

DL1.1.14. Certification Test and Evaluation (CT&E). Software and hardware security tests conducted during the development of the IS.

DL1.1.15. Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

DL1.1.16. Compartmented Mode. INFOSEC mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all the following:

DL1.1.16.1. Valid security clearance for the most restricted information processed in the system;

DL1.1.16.2. Formal access approval and signed nondisclosure agreements for that information which a user is to have access; and

DL1.1.16.3. Valid need-to-know for information which a user is to have access.

DL1.1.17. Computer Security (COMPUSEC). Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated.

DL1.1.18. Computing Environment. The total environment in which an automated information system (IS), network, or a component operates. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other ISs.

DL1.1.19. Confidentiality. Assurance that information is not disclosed to unauthorized persons, processes, or devices.

DL1.1.20. Configuration Control. Process of controlling modifications to hardware, firmware, software, and documentation to ensure that the IS is protected against improper modifications prior to, during, and after system implementation.

DL1.1.21. Configuration Management. Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IS.

DL1.1.22. Configuration Manager. The individual or organization responsible for configuration control or configuration management.

DL1.1.23. Data Integrity. Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

DL1.1.24. Dedicated Mode. IS security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:

DL1.1.24.1. Valid security clearance for all information within the system;

DL1.1.24.2. Formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments and/or special access programs); and

DL1.1.24.3. Valid need-to-know for all information contained within the IS. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

DL1.1.25. Defense Information Infrastructure (DII). The DII encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the Department of Defense's local and worldwide information needs. The DII connects DoD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and provides information processing and value-added services to subscribers over the Defense Information Systems Network (DISN). Unique user data, information, and user applications software are not considered part of the DII.

DL1.1.26. Designated Approving Authority (DAA or Accreditor) Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designed accrediting authority and delegated accrediting authority.

DL1.1.27. Developer. The organization that develops the IS.

DL1.1.28. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD process for identifying information security requirements, providing security solutions, and managing IS security activities.

DL1.1.29. Emissions Security (EMSEC). Protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from crypto-equipment or an IS.

DL1.1.30. Environment. Aggregate of external procedures, conditions, and objects effecting the development, operation, and maintenance of an IS.

DL1.1.31. Evolutionary Program Strategies. Generally characterized by design,

development, and deployment of a preliminary capability that includes provisions for the evolutionary addition of future functionality and changes, as requirements are further defined (reference (i)).

DL1.1.32. Governing Security Requisites. Those security requirements that must be addressed in all systems. These requirements are set by policy, directive, or common practice set; e.g., by Executive Order, Office of Management and Budget (OMB), Office of the Secretary of Defense, a Military Service or DoD Agency. Governing security requisites are typically high-level requirements. While implementations will vary from case to case, these requisites are fundamental and must be addressed.

DL1.1.33. Grand Design Program Strategies. Characterized by acquisition, development, and deployment of the total functional capability in a single increment (reference (i)).

DL1.1.34. Incremental Program Strategies. Characterized by acquisition, development, and deployment of functionality through a number of clearly defined system "increments" that stand on their own (reference (i)).

DL1.1.35. Information Assurance (IA). Information operations protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of ISs by incorporating protection, detection, and reaction capabilities.

DL1.1.36. Information Assurance Support Environment (IASE). The IASE is an on-line web-based help environment for DoD INFOSEC and IA professionals.

DL1.1.37. Information Category. The term used to bind information and tie it to an information security policy.

DL1.1.38. Information Operations. Actions taken to affect adversary information and ISs while defending one's own information and ISs.

DL1.1.39. Information Security Policy. The aggregate of directives, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information. For example, the information security policy for financial data processed on DoD systems can be contained in Public Laws, Executive Orders, DoD Directives, and local regulations. The information security policy should also list all the security requirements applicable to specific information.

DL1.1.40. Information System (IS). The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

DL1.1.41. Information System Security (INFOSEC). Protection of ISs against unauthorized access to information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

DL1.1.42. Information System Security Officer (ISSO). The person responsible to the DAA for ensuring the security of an IS throughout its life cycle, from design through disposal. Synonymous with system security officer.

DL1.1.43. Information Technology (IT). The hardware, firmware, and software used as part of the IS to perform DoD information functions. This definition includes computers, telecommunications, automated ISs, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

DL1.1.44. Infrastructure-centric. A security management approach that considers ISs and their computing environment as a single entity.

DL1.1.45. Integrator. The organization that integrates the IS components.

DL1.1.46. Integrity. Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

DL1.1.47. Interim Approval To Operate (IATO). Temporary approval granted by a DAA for an IS to process information based on preliminary results of a security evaluation of the system.

DL1.1.48. Legacy Information System. An operational IS that existed prior to the implementation of the DITSCAP.

DL1.1.49. Maintainer. The organization that maintains the IS.

DL1.1.50. Maintenance Organization. The Government organization responsible for the maintenance of an IS. (Although the actual organization performing maintenance on a system may be a contractor, the maintenance organization is the Government organization responsible for the maintenance.)

DL1.1.51. Mission. The assigned duties to be performed by a resource.

DL1.1.52. Mission Justification. The description of the operational capabilities required to perform an assigned mission. This includes a description of a system's capabilities, functions, interfaces, information processed, operational organizations supported, and the intended operational environment.

DL1.1.53. Non-Developmental Item (NDI). Any item that is available in the commercial marketplace; any previously developed item that is in use by a Department or Agency of the United States, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; any item described above that requires only minor modifications in order to meet the requirements of the procuring Agency; or any item that is currently being produced that does not meet the requirements of definitions above, solely because the item is not yet in use or is not yet available in the commercial marketplace.

DL1.1.54. Multilevel Mode. INFOSEC mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts:

DL1.1.54.1. Some users do not have a valid security clearance for all the information processed in the IS;

DL1.1.54.2. All users have the proper security clearance and appropriate formal access approval for that information to which they have access; and

DL1.1.54.3. All users have a valid need-to-know only for information for which they have access.

DL1.1.55. Operational Security (OPSEC). Process denying information to adversaries about capabilities and/or intentions by identifying, controlling, and protecting unclassified generic activities.

DL1.1.56. Other Program Strategies. Strategies intended to encompass variations and/or combinations of the grand design, incremental, evolutionary, or other program strategies (reference (i)).

DL1.1.57. Passive System. A system related indirectly to other systems. Passive systems may or may not have a physical connection to other systems, and their logical connection is controlled tightly.

DL1.1.58. Program Manager. The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IS.

DL1.1.59. Residual Risk. Portion of risk remaining after security measures have been applied.

DL1.1.60. Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.

DL1.1.61. Risk Assessment. Process of analyzing threats to and vulnerabilities of an IS and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and cost-effective measures.

DL1.1.62. Risk Management. Process concerned with the identification, measurement, control, and minimization of security risks in ISs to a level commensurate with the value of the assets protected.

DL1.1.63. Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

DL1.1.64. Security Inspection. Examination of an IS to determine compliance with security policy, procedures, and practices.

DL1.1.65. Security Process. The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life cycle.

DL1.1.66. Security Requirements. Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

DL1.1.67. Security Requirements Baseline. Description of the minimum requirements necessary for an IS to maintain an acceptable level of security.

DL1.1.68. Security Specification. Detailed description of the safeguards required to protect an IS.

DL1.1.69. Security Test and Evaluation (ST&E). Examination and analysis of the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of that system.

DL1.1.70. Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (Privacy Act) (reference (at)), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (reference (c)).

DL1.1.71. System. The set of interrelated components consisting of mission, environment, and architecture as a whole.

DL1.1.72. System Entity. A system subject (user or process) or object.

DL1.1.73. System Integrity. The attribute of an IS when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

DL1.1.74. System High Mode. IS security mode of operation wherein each user, with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts, has all of the following:

DL1.1.74.1. Valid security clearance for all information within an IS;

DL1.1.74.2. Formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments and/or special access programs); and

DL1.1.74.3. Valid need-to-know for some of the information contained within the IS.

DL1.1.75. System Security Authorization Agreement (SSAA). The SSAA is a formal agreement among the DAA(s), the Certifier, user representative, and program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify IA requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

DL1.1.76. TEMPEST. Short name referring to investigation, study, and control of compromising emanations from IS equipment.

DL1.1.77. Threat. Any circumstance or event with the potential to harm an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

DL1.1.78. Threat Assessment. Formal description and evaluation of threat to an IS.

DL1.1.79. Trusted Computing Base (TCB). Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

DL1.1.80. User. Person or process authorized to access an IS.

DL1.1.81. User Representative. The individual or organization that represents the user or user community in the definition of IS requirements.

DL1.1.82. Validation Phase. The users, acquisition authority, and DAA agree on the correct implementation of the security requirements and approach for the completed IS.

DL1.1.83. Verification Phase. The process of determining compliance of the evolving IS specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and DAA.

DL1.1.84. Vulnerability. Weakness in an IS, system security procedures, internal controls, implementation that could be exploited.

DL1.1.85. Vulnerability Assessment. Systematic examination of an IS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

AL1. ABBREVIATIONS AND/OR ACRONYMS

AL1.1. AIS	Automated Information System
AL1.2. ASAP	As soon as possible
AL1.3. C&A	Certification and Accreditation
AL1.4. CDR	Critical Design Review
AL1.5. CM	Configuration Management
AL1.6. COMPUSEC	Computer Security
AL1.7. COMSEC	Communications Security
AL1.8. CONOPS	Concept of Operations
AL1.9. COTS	Commercial Off-The-Shelf
AL1.10. CRR	Certification Requirements Review
AL1.11. DAA	Designated Approving Authority
AL1.12. DAC	Discretionary Access Controls
AL1.13. DCID	Director of Central Intelligence Directive
AL1.14. DGSA	DoD Goal Security Architecture
AL1.15. DITSCAP	DoD Information Technology Security Certification and Accreditation Process
AL1.16. DISN	Defense Information System Network
AL1.17. DISSP	Defense Wide Information Systems Security Program
AL1.18. DODIIS	Department of Defense Intelligence Information System
AL1.19. DoD	Department of Defense
AL1.20. DT&E	Developmental Test and Evaluation
AL1.21. EPL	Evaluated Product List
AL1.22. EPROM	Erasable Programmable Read-Only Memory
AL1.23. ERTZ	Electromagnetic Radiation TEMPEST Zone
AL1.24. EMSEC	Emissions Security
AL1.25. FCA	Functional Configuration Audit
AL1.26. FIPS	Federal Information Processing Standard
AL1.27. GOTS	Government Off-The-Shelf
AL1.28. IA	Information Assurance
AL1.29. IASE	Information Assurance Support Environment
AL1.30. IATO	Interim Approval To Operate
AL1.31. INFOSEC	Information Systems Security
AL1.32. IOT&E	Initial Operational Test and Evaluation
AL1.33. ISSO	Information Systems Security Officer
AL1.34. IS	Information System
AL1.35. IT	Information Technology
AL1.36. IV&V	Independent Verification and Validation
AL1.37. LAN	Local Area Network

AL1.38.	LCM	Life-Cycle Management
AL1.39.	MAIS	Major Automated Information System
AL1.40.	MDAPS	Mandatory Procedures for Major Defense Programs
AL1.41.	MILDEP	Military Department
AL1.42.	MIL-STD	Military Standard
AL1.43.	NATO	North Atlantic Treaty Organization
AL1.44.	NCSC	National Computer Security Center
AL1.45.	NDI	Non-Developmental Item
AL1.46.	NIST	National Institute of Standards and Technology
AL1.47.	NSA	National Security Agency
AL1.48.	NSTISSAM	National Security Telecommunications and Information Systems Security Advisory Memorandum
AL1.49.	NSTISSI	National Security Telecommunications and Information Systems Security Instruction
AL1.50.	NSTISSIC	National Security Telecommunications and Information Systems Security Committee
AL1.51.	NSTISSI 4009	National Telecommunications and Information Systems Security (INFOSEC) Glossary
AL1.52.	NOFORN	No Foreign Dissemination
AL1.53.	OMB	Office of Management and Budget
AL1.54.	OPSEC	Operational Security
AL1.55.	O/S	Operating System
AL1.56.	PCA	Physical Configuration Audit
AL1.57.	PCS	Physical Control Space
AL1.58.	PDR	Preliminary Design Review
AL1.59.	PROM	Programmable Read-Only Memory
AL1.60.	P. L.	Public Law
AL1.61.	RTM	Requirements Traceability Matrix
AL1.62.	SCI	Sensitive Compartmented Information
AL1.63.	SCIF	Sensitive Compartmented Information Facility
AL1.64.	SFUG	Security Features Users Guide
AL1.65.	SIOP-ESI	Single Integrated Operations Plan - Extremely Sensitive Information
AL1.66.	SSAA	System Security Authorization Agreement
AL1.67.	ST&E	Security Test and Evaluation
AL1.68.	TCB	Trusted Computing Base
AL1.69.	TCSEC	Trusted Computer Security Evaluation Criteria
AL1.70.	TFM	Trusted Facility Manual
AL1.71.	WAN	Wide Area Network

C1. CHAPTER 1

INTRODUCTION

C1.1. BACKGROUND

C1.1.1. The Office of Assistant Secretary of Defense directed the Defense Wide Information Systems Security Program (DISSP) to create standardized requirements and processes for accreditation of computers, systems and networks in its August 19, 1992, memorandum, "The Defense Information Systems Security Program," (reference (a)). A security process improvement working group was formed to develop this standard process. Their task was to develop a standard certification and accreditation (C&A) process that would meet the policies defined in DoD Directive 5200.28, Public Law (P.L.) 100-235 (1988), Office of Management and Budget (OMB) Circular A-130, Appendix III, Director of Central Intelligence (DCID) 1/16 and DoD Directive 5220.22 (references (b) through (f)).

C1.1.2. DoD Directive 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)" (reference (g)), established the DITSCAP as the standard C&A process for the Department of Defense. This Manual supports the DITSCAP by presenting a detailed approach to the activities comprising the C&A process. This Manual provides standardized activities leading to accreditation and establishes a process and management baseline. C&A assistance may be obtained from the DoD Information Assurance Support Environment (IASE). The IASE provides both self-help and assisted help in implementing uniform C&A practices and describes in detail how to execute the C&A activities. Unclassified users [1] may access the IASE at http://iase.disa.mil or by e-mail to ASE@ncr.disa.mil. Classified users may access the IASE on the SIPRNet at http://cassie.iiie.disa.smil.mil or by e-mail to IASE@iiie.disa.smil.mil.

C1.1.3. The DITSCAP Application Manual is a stand-alone reference manual or handbook. Chapter 1 provides an introduction to the DITSCAP, Chapter 2 is an overview of the security process. Each phase of the DITSCAP is composed of activities. Some activities have subordinate tasks. Chapter 3 provides a detailed description of the DITSCAP Phase 1 activities and tasks. Chapters 4, 5, and 6 provide similar information for Phases 2, 3, and 4. Chapter 7 describes the DITSCAP

---

[1] Only users with .mil or .gov accounts are permitted to access the IASE.

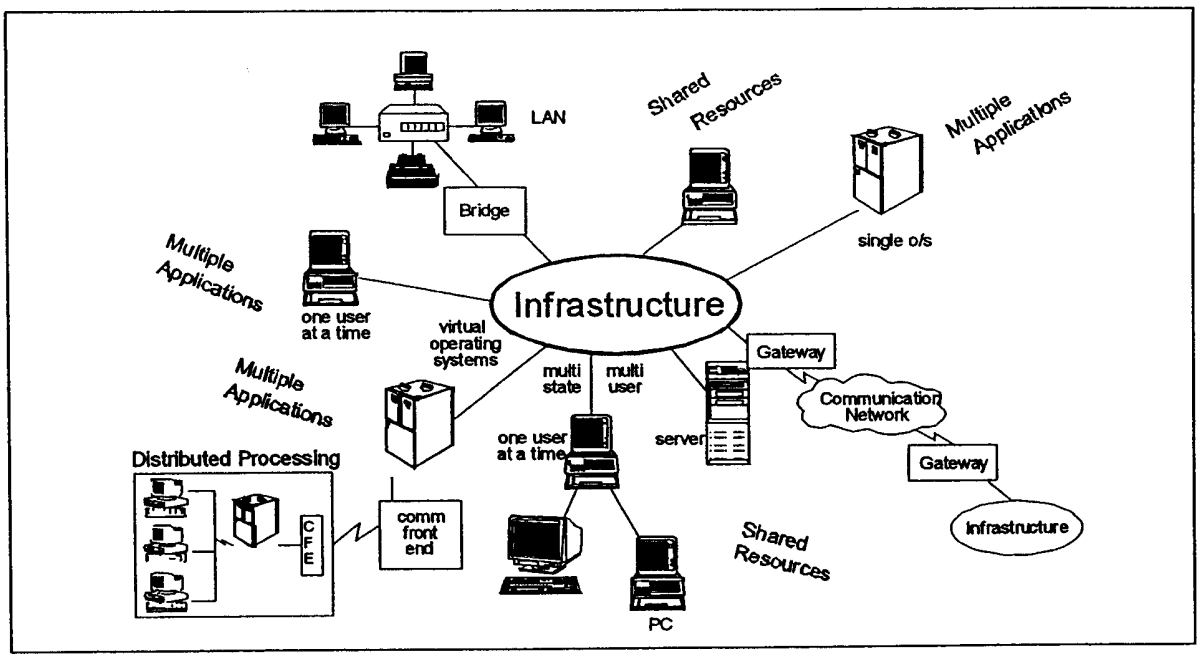
relationship to a system life cycle. Chapter 8 is a summary of management roles and responsibilities.

C1.2. TECHNOLOGY OVERVIEW

C1.2.1. Within the Department of Defense, IS and networks perform a wide variety of functions. Ever increasing reliance is being placed on these systems, regardless of their classifications, to accomplish the DoD missions. The information and processes must be protected to ensure an appropriate level of confidentiality, integrity, availability, and accountability and to ensure that Defense operations are not disrupted and DoD missions are accomplished. When properly administered, the level of protection is based on the value of the information to the mission of the Agency and the value of its IS resources. The value of the information is related to the adverse impact that the loss of, alteration of, denial of access to, or unauthorized access to information would have on the Department of Defense in accomplishing its missions. The value that the Department of Defense and national-level decision makers place on this information is manifested through the current security policies and procedures established through public laws and national and DoD regulatory publications.

C1.2.2. DoD Directive 5200.28, reference (b), mandates the accreditation of automated information systems (IS), to include stand-alone personal computers, connected systems, and networks. The interpretation and implementation of this Directive varies across Service and Agency boundaries. As shown in Figure C1.F1., information technology has become more complex.

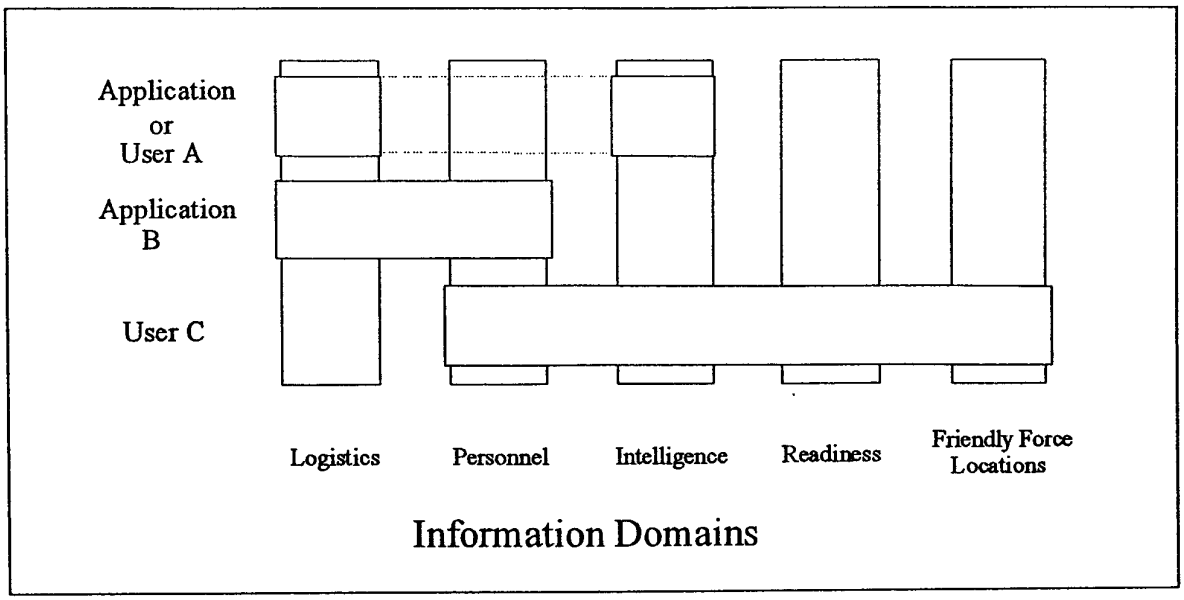
Figure C1.F1. Information Infrastructure



C1.2.3. Technological advances now enable DoD IS users to process information at various locations and to access it from anywhere in the world. These technological advances and a shrinking budget have collapsed the DoD infrastructure, caused information and processes to be distributed, and information to flow across systems. The challenge is to provide an effective level of security, in a distributed and interconnected environment, consistent with functional needs and within budget constraints.

C1.2.4. Figure C1.F2. illustrates information access requirements. Users and processes must be able to access information of different classifications and sensitivities across information categories and domains. Information may be spread across multiple sites or systems. The sites may be different Services or Agencies. The users may be other IS. In some cases the information and the users may be collocated; however, frequently they are dispersed. Security controls must manage information sharing among different user communities. Information security has become a global responsibility with universal consequences.

Figure C1.F2. User Information Access Requirements



C1.2.5. The DITSCAP applies to C&A professionals, users, acquisition and maintenance organizations, developers, system integrators and procurement officials. Each of these communities has a specific role in developing, procuring, employing and operating an IS with an acceptable level of residual risk.

C1.3. DITSCAP OBJECTIVE

The DITSCAP establishes a standard process, set of activities, general tasks, and a management structure to certify and accredit IS that will maintain the information assurance (IA) and security posture of the Defense Information Infrastructure (DII). This process supports an infrastructure-centric approach, with a focus on the mission, environment, and architecture. For a system in development, the intent is to identify appropriate security requirements, design to meet those requirements, test the design against the same requirements, and then monitor the accredited system for changes or reaccredidation as necessary.

C1.4. DITSCAP CHARACTERISTICS

C1.4.1. A C&A process must be applicable to all DoD environments. It must be capable of assessing the security posture of an individual system and the effect of each system on the security posture of every other system in its computing environment. The security process must be sufficiently flexible to evaluate systems in various life-cycle stages, systems under evolutionary development, and those single purpose or legacy systems for as long as they exist.

C1.4.2. There are nine characteristics that provide the flexibility needed to support the diverse DoD mission requirements. A process with these characteristics is essential to integrating information security into the developmental and operational processes of the next generation of DoD systems. This process will permit IS to be evaluated based on mission versus risk in a computing environment where the systems are interdependent and, frequently, interactive. The DITSCAP has these nine characteristics. These characteristics are:

C1.4.2.1. Tailorable. The process is applicable to any system regardless of the system status in its life cycle or shift in program strategy. The life cycle continues until the system is removed from DoD service. The process may be applied to any program strategy (grand design, incremental, or evolutionary).

C1.4.2.2. Scalable. The process is applicable to systems differing in security requirements, size, complexity, connectivity, and data policies.

C1.4.2.3. Predictable. The process is uniformly applicable to any system. It minimizes personal opinion and subjectivity.

C1.4.2.4. Understandable. The process provides the participants with a consistent view of the security requirement compliance of the system.

C1.4.2.5. Relevant. The process facilitates the identification of security requirements and solutions that are achievable (available, affordable, and within the context of the development approach, IA strategies, and mission needs).

C1.4.2.6. Effective. The process results in and maintains an accreditation for the target system.

C1.4.2.7. Evolvable. The process allows for the incorporation of lessons learned, as well as changes in security policy and technology, in a manner that meets the time schedule of the mission.

C1.4.2.8. Repeatable. The process provides corresponding results when applied or reapplied to similar IS.

C1.4.2.9. Responsive. The process accommodates timely responses essential for supporting emergent Military Department (MILDEP) and national operational requirements and priorities.

C2. CHAPTER 2

THE SECURITY PROCESS

C2.1. SECURITY PROCESS OVERVIEW

C2.1.1. C&A Process. Chapters 3 through 6 describe a process that standardizes all activities leading to a successful accreditation. The principal purpose of the process is to protect and secure the entities comprising the DII with a proper balance between the benefits to the operational missions, the risks to those same missions, and the life-cycle costs. Standardizing the process helps to ensure that the shared interests of the common infrastructure are approximately represented and accounted for in the decision-making process. The DITSCAP, Figure C2.F1., consists of the Definition, Verification, Validation, and Post Accreditation Phases.

C2.1.1.1. Phase 1, Definition. The Definition Phase includes activities to verify the system mission, environment and architecture, identify the threat, define the levels of effort, identify the Designated Approving Authority [2] (DAA) and Certification Authority (Certifier), and document the C&A security requirements. Phase 1 culminates with a documented agreement between the Program Manager, DAA, Certifier, and user representative on the approach and results of the Phase 1 activities.

C2.1.1.2. Phase 2, Verification. The Verification Phase includes activities to document compliance of the system with previously agreed on security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (h)), there is a corresponding set of security activities that verifies compliance with the security requirements and constraints and evaluates vulnerabilities.

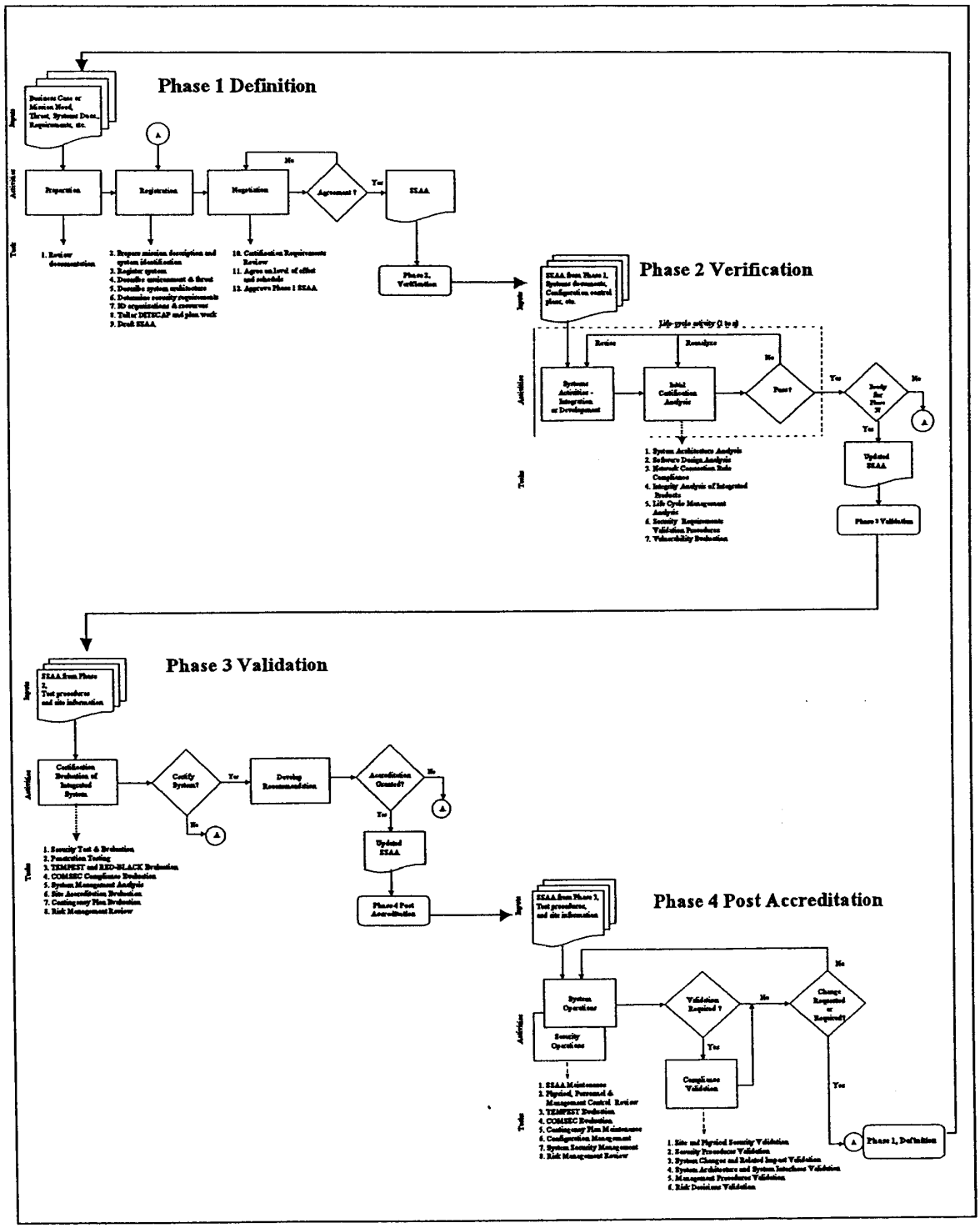
C2.1.1.3. Phase 3, Validation. The Validation Phase includes activities to assure the fully integrated system in its specific operating environment and configuration provides an acceptable level of residual risk. Validation culminates in an approval to operate.

---

[2] The DAA is also referred to as the Accreditor throughout this Manual.

C2.1.1.4. Phase 4, Post Accreditation. The Post Accreditation Phase includes activities to monitor system management, configuration, and changes to the operational and threat environment to ensure an acceptable level of residual risk is preserved. Security management, configuration management, and periodic compliance validation reviews are conducted. Changes to the system environment or operations may warrant beginning a new DITSCAP cycle.

Figure C2.F1. Overview of the DITSCAP Phases



C2.1.1.5. DITSCAP uses a single document approach. All the information relevant to the C&A is collected into the one document, the Systems Security Authorization Agreement (SSAA). The SSAA is designed to fulfill the requirements of OMB Circular No. A-130 (reference (d)) for a security plan and to meet all the needs for C&A support documentation.

C2.1.1.6. The key to the DITSCAP is the agreement between the program manager,[3] DAA, Certifier, and user representative. These individuals resolve critical schedule, budget, security, functionality, and performance issues. This agreement is documented in the SSAA. The SSAA is used to guide and document the results of the C&A. The objective is to use the SSAA to establish an evolving, yet binding, agreement on the level of security required before the system development begins or changes to a system are made. After accreditation, the SSAA becomes the baseline security configuration document.

C2.1.2. Life-Cycle and Tailoring. The DITSCAP process applies to all systems requiring C&A throughout their life cycle. It is designed to be adaptable to any type of any IS and any computing environment and mission. It may be adapted to include existing system certifications, evaluated products, new security technology or programs and adjusted to the applicable standards. The DITSCAP may be mapped to any system life-cycle process but is independent of the life-cycle strategy. The DITSCAP is designed to adjust to the development, modification, and operational life-cycle phases. Each new C&A effort begins with Phase 1, Definition, and ends with Phase 4, Post Accreditation, in which follow-up actions ensure that the approved IS or system component continues to operate in its computing environment according to its accreditation. The activities defined in these four phases are mandatory. However, implementation details of these activities may be tailored and, where applicable, integrated with other acquisition activities and documentation.

---

[3] Program manager is used in this Manual to refer to the acquisition organization's program manager during the system acquisition, the system manager during operation of the system, or the maintenance organization's program manager when a system is undergoing a major change.

C2.1.3. Certification Levels. The DITSCAP certification tasks must be performed at one of four certification levels. To determine the appropriate level of certification, the Certifier must analyze the system business functions, national, DoD, and Agency security requirements, criticality of the system to the organization's mission, software products, computer infrastructure, data processed by the system, and types of users. Considering this information, the Certifier determines the degree of confidentiality, integrity, availability, and accountability required for the system. Based on this analysis, the Certifier recommends a certification level: Level 1 – basic security review, Level 2 – minimum analysis, Level 3 – detailed analysis, or Level 4 – comprehensive analysis. The DITSCAP certification tasks must be performed at one of these four levels of certification.

C2.2. RISK MANAGEMENT

C2.2.1. Background. Risk management is the total process of identifying, measuring, controlling, and minimizing or reducing the security risk incurred by an IS to a level commensurate with the value of the assets protected. Risks are generally defined as the coexistence of a threat and a vulnerability. NSTISSI 4009, reference (j), defines a threat as "any circumstance or event with the potential to cause harm to an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service." Reference (j) also defines vulnerability as "a weakness in an IS, system security procedures, internal controls, or implementation that could be exploited." Threats exist at many levels, but may pose little concern unless there is a vulnerability that may be exploited by that threat. Either eliminating or reducing the capabilities of the threat agent or the corresponding vulnerability may reduce a risk. The goal is to obtain what OMB Circular No. A-130 (reference (d)), defines as "adequate security." Reference (d) defines adequate security as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act. NIST Special Publication 800-12, "An Introduction to Computer Security," reference (k), provides additional insight into risk management.

C2.2.1.1. Risk Assessment and Identification. Risks may be identified during normal operations or as the result of a C&A effort, risk analysis, or an incident. Reference (c) no longer requires the preparation of formal risk analysis or assessment. In the past substantial resources have been expended preparing complex analyses of systems with limited tangible benefit in terms of improved security for the

IS. Rather than try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them. While formal risk assessments need not be preformed, the need to determine adequate security will require that a risk-based approach be used. This risk approach should consider the major factors in risk management, the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

C2.2.1.2. The DITSCAP C&A effort is structured to first develop a threat assessment. Then, as a result of Phase 2 and 3 analysis and testing, vulnerabilities will be identified. The Phase 2 Vulnerability Assessment Task provides guidance to evaluate the vulnerabilities. Similarly vulnerabilities may be identified as a result of a security incident.

C2.2.2. Risk Management Concept. After the threats and vulnerabilities are identified, reducing the vulnerability or the threat must minimize the risk. The best management procedures will thoroughly evaluate the risk in light of potential safeguards. Alternative risk abatement measures should be considered in the light of cost versus risk.

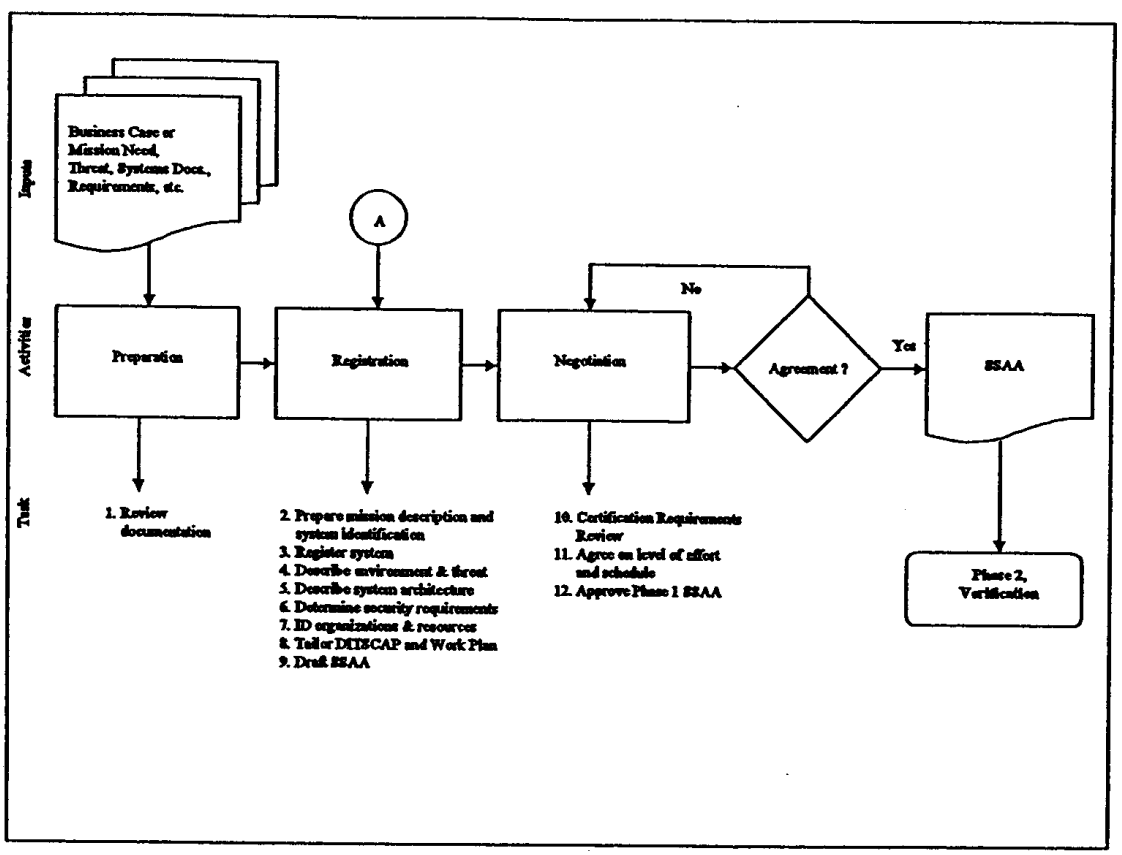
C3. CHAPTER 3

PHASE 1, DEFINITION

C3.1. PHASE 1 OVERVIEW

C3.1.1. Phase 1 initiates the DITSCAP process by acquiring or developing the information necessary to understand the IS under evaluation and then using that information to plan the C&A tasks. The objectives of the Phase 1 activities, Figure C3.F1., are to agree on the intended system mission, security requirements, C&A boundary, level of effort, and resources required.

Figure C3.F1. Definition Activities



C3.1.2. Phase 1 tasks define the C&A level of effort, identify the principal C&A roles and responsibilities, and culminate with an agreement on the method for implementing the security requirements. This agreement is documented in the

SSAA. The SSAA also describes the applicable set of planning and certification actions, resources, and documentation required for the C&A. The SSAA outline, Appendix 1, lists information that should be included.

C3.1.3. Phase 1 starts when an IS is developed or modified in response to a business case, operational requirement, mission needs, or significant change in threat. The activities provide an understanding of the IS, document the security requirements, develop a security architecture approach, and determine the scope, level of effort, documentation required, and schedule for the certification actions. Any change to existing systems initiates the DITSCAP. During the registration and negotiation activities the program manager, DAA, Certifier, and user representative determine what actions are required in response to the system change.

C3.2. SSAA OVERVIEW

C3.2.1. The SSAA is a formal agreement among the DAA(s), Certifier, user representative, and program manager. The SSAA is used throughout the entire DITSCAP process to guide actions, document decisions, specify IA requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational systems security. The characteristics of an SSAA are listed in Table C3.T1.

Table C3.T1. SSAA Characteristics

1.	Describes the operating environment and threat.
2.	Describes the system security architecture.
3.	Establishes the C&A boundary of the system to be accredited.
4.	Documents the formal agreement among the DAA(s), Certifier, user representative, and program manager.
5.	Documents all requirements necessary for accreditation.
6.	Documents all security criteria for use throughout the IS life cycle.
7.	Minimizes documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations, architecture description, etc.).
8.	Documents the DITSCAP plan.
9.	Documents test plans and procedures, certification results, and residual risk.
10.	Forms the baseline security configuration document.

C3.2.2. Each IS must be covered by an SSAA. In some cases a single SSAA may include several systems. For type accreditation's, an SSAA may be prepared for the system software and hardware considered under the type accreditation. This SSAA

should be shipped to each prospective installation site with the software and hardware. In this situation, the site manager will receive confirmation and documentation of the C&A results and the equipment included in the SSAA. After installation of the IS, the information from the type SSAA should be included in the target system's (network or site) SSAA. The system configuration and security environment must still be certified during Phase 3.

C3.2.3. The physical characteristics of the SSAA will depend on the certification complexity and organizational requirements. The SSAA can be a single document or a complex document with multiple appendices and enclosures. The goal is to produce an SSAA that will be the basis of agreement throughout the system's life cycle. The SSAA is intended to consolidate security related documentation into one document. This eliminates the redundancy and potential confusion caused by multiple documents to describe the system, security policy, system and security architecture, etc. When feasible, the SSAA may be tailored to incorporate other documents as appendices or by reference.

C3.2.4. The DAA, Certifier, user representative, and program manager have the authority to tailor the SSAA to meet the characteristics of the IS, operational requirements, security policy, and prudent risk management. The SSAA format is flexible enough to permit adjustment throughout the system's life cycle as conditions warrant. New requirements may emerge from design necessities, existing requirements may need to be modified, or the DAA's overall view of acceptable risk [4] may change. When that occurs, the SSAA is updated to accommodate the new components. Either the program manager or Certifier develops the SSAA in Phase 1. It is updated in each phase as the system development progresses and new information becomes available. In this sense, the SSAA is a living document. The completed SSAA contains those items that must be agreed to by the DAA, Certifier, user representative, and program manager.

C3.2.5. The SSAA must identify all costs relevant to the C&A process. The program manager must add a C&A funding line item to the program budget to ensure the funds are available. Funding must cover any contractor support, travel, or test tool costs associated with certification, test development, testing and accreditation. The SSAA is a binding agreement among Government and Government contractor entities. The provisions for developing and implementing the SSAA must be included in contractual documents between the Government and its contractors.

---

4 Acceptable risk must consider the balance between the benefits derived from the use of the system, the risks posed to both the system and community users, and the costs required to alleviate the risks.

C3.3. PHASE 1 ACTIVITIES

C3.3.1. Phase 1 contains three activities: preparation, registration, and negotiation. Any security related changes should initiate the DITSCAP process for any existing or legacy IS. When the DITSCAP process is initiated for legacy systems, the available C&A documentation should be converted to the SSAA format.

C3.3.2. Preparation. The DITSCAP process starts when an IS is developed or modified in response to a business case, operational requirements, mission needs, or significant change in threats to be countered. During the preparation activity, information and documentation is collected about the system. This information includes capabilities and functions the system will perform, desired interfaces and data flows associated with those interfaces, information to be processed, operational organizations supported, intended operational environment, and operational threat. Typically, this information is contained in the business case or mission needs statement, system specifications, architecture and design documentation, user manuals, operating procedures, network diagrams, and configuration management documentation, if available. National, Agency, and organizational-level security instructions and policies should also be reviewed. Table C3.T2. identifies the types of information collected and reviewed during the preparation activity.

Table C3.T2. Materials Reviewed During Preparation

1.	Business Case
2.	Mission Needs Statement
3.	System Specifications
4.	Architecture and Design Documents
5.	User Manuals
6.	Operating Procedures
7.	Network Diagrams
8.	Configuration Management Documents
9.	Threat Analysis
10.	Federal and Organizational IA and Security Instructions and Policies

C3.3.3. Registration. Registration initiates the risk management agreement process among the program manager, DAA, Certifier, and user representative. Information is evaluated, applicable IA requirements [5] are determined, risk management and vulnerability assessment actions begin, and the level of effort required for C&A is determined and planned. Registration begins with preparing the system description and system identification and concludes with preparing an initial draft of the SSAA.

C3.3.3.1. Registration tasks guide the evaluation of information necessary to address the risk management process in a repeatable, understandable, and effective manner. Registration tasks identify security requirements and the level of effort required to complete the C&A. The requirements and level of effort are guided by the degree of assurance needed in the areas of confidentiality, integrity, availability, and accountability. Registration tasks consider the system development approach, system life-cycle stage, existing documentation, system business functions, environment (including the threat assessment), architecture, users, data classification and categories, external interfaces, and mission criticality. The registration tasks are listed in Table C3.T3.

Table C3.T3. Registration Tasks

1.	Prepare business or operational functional description and system identification.
2.	Inform the DAA, Certifier, and user representative that the system will require C&A support (register the system).
3.	Prepare the environment and threat description.
4.	Prepare system architecture description and describe the C&A boundary.
5.	Determine the system security requirements.
6.	Tailor the DITSCAP tasks, determine the C&A level of effort, and prepare a DITSCAP plan.
7.	Identify organizations that will be involved in the C&A and identify resources required.
8.	Develop the draft SSAA.

C3.3.3.2. A key registration task is to prepare a description of the accreditation boundary (system boundary, facilities, equipment, etc.) and the external interfaces with other equipment or systems. The accreditation boundary should include all IS equipment that is to be addressed in the C&A. The IS facility and

---

[5] National and DoD-level guidance define IA requirements. Additional IA requirements may be defined by each Service or Agency or may be developed from International Standard 15408, the Common Criteria.

equipment must be under the control of the DAA. Any facility or equipment that is not considered or is not under the control of the DAA should be considered as external interfaces.

C3.3.3.3. Currently known threats should be assessed against the specific business functions and system description to determine the required protection. The threat, and subsequent vulnerability assessments, must be used in establishing and selecting the IA policy objectives that will counter the threat.

C3.3.3.4. The DITSCAP has four levels of certification to provide the flexibility for appropriate assurance within schedule and budget limitations. To determine the appropriate level of certification, the Certifier must analyze the system business functions, national, DoD, and Service or Agency security requirements, criticality of the system to the organizations mission, software products, computer infrastructure, data processed by the system, and types of users. Considering this information, the Certifier determines the degree of confidentiality, integrity, availability, and accountability required for the system. Based on this analysis, the Certifier recommends a certification level: Level 1 - basic security review, Level 2 – minimum analysis, Level 3 – detailed analysis, or Level 4 – comprehensive analysis. The DITSCAP certification tasks must be performed at one of these four levels of certification.

C3.3.3.5. The DITSCAP should be tailored to address the specific needs of the system, security requirements, and program requirements. For example, if a type accreditation is planned, a Certification Test and Evaluation (CT&E) may be added to Phase 2. The corresponding Phase 3 Security Test and Evaluation (ST&E) must then be tailored to provide the necessary assurance that the type accredited software and/or hardware is correctly installed in an operational environment that completes the specified requirements. The type accreditation SSAA must also be tailored to fit the type accreditation concept. The type accreditation SSAA should document the CT&E results in the SSAA and define the intended operating environment as well as any restrictions or operating procedures required for the type accredited system. The type accredited SSAA should be delivered to each operating site with the type accredited system. The site managers may then include the type accreditation in their C&A process without repeating the software and hardware tests for the type accredited system.

C3.3.3.6. The SSAA is prepared during the registration activities. When registration activities are concluded, the Certifier submits a draft SSAA to the DAA,

program manager, and user representative. The draft SSAA is then used as the basis for discussions during the negotiation activity.

C3.3.4. Negotiation. During negotiation all the participants [6] involved in the IS's development, acquisition, operation, security certification, and accreditation reach agreement on the implementation strategy to be used to satisfy the security requirements identified during system registration. The negotiation tasks are shown in Table C3.T4.

Table C3.T4. Negotiation Tasks

1.	Conduct the Certification Requirements Review (CRR).
2.	Agree on the security requirements, level of effort, and schedule.
3.	Approve final Phase 1 SSAA.

C3.3.4.1. Negotiation starts with a review of the draft SSAA. The DAA conducts a complete review of the draft SSAA to determine that all applicable IA and security requirements are included. The Certifier conducts an evaluation of the technical and non-technical security features of the IS based on the negotiated certification level of effort. The Certifier is the technical expert that documents tradeoffs between security requirements, cost, availability, and schedule to manage security risk. The program manager reviews the SSAA for accuracy, completeness, costs, and schedule considerations. The user representative reviews the SSAA to determine if the system will support the user's mission and that appropriate security operating procedures will be available at system delivery. All participants review the proposed certification level and resource requirements to determine that the appropriate assurance is being applied.

C3.3.4.2. A CRR must be held for the C&A participants. The CRR review must result in an agreement regarding the level of effort and the approach that will be taken to implement the security requirements. The review must include the information documented in the SSAA (mission and system information, operational and security functionality, operational environment, security policy, system security requirements, known security problems or deficiencies, and other security relevant information).

---

[6] These individuals may choose to designate someone to represent them in the negotiations. (In some cases, the DAA may designate the Certifier to act in his or her behalf.) Unless noted, the terms will be used interchangeably to mean the principle or their designated representative and the staff that supports them.

C3.3.4.3. The purpose of negotiation is to ensure that the SSAA properly and clearly defines the approach and level of effort. During negotiation, all participants must develop an understanding of their roles and responsibilities. Negotiation ends when the responsible organizations adopt the SSAA and concur that those objectives have been reached.

C3.4. PHASE 1 TASKS

Throughout this Manual the DITSCAP tasks are be numbered using the convention where the first number indicates the phase of the DITSCAP where the task is performed and the second number is the number of the task in that phase. For example, Task 2-1 is the first task in phase 2.

C3.4.1. Task 1-1, Review Documentation.

C3.4.1.1. Task Objective. The objective of this task is to obtain and review documentation relevant to the system.

C3.4.1.2. Task Description. In the review documentation task, information and documentation is collected about the system. This information includes capabilities and functions the system will perform, operational organizations supported, intended operational environment, and operational threat. Typically, this information is contained in the business case or mission needs statement, system specifications, architecture and design documentation, user manuals, operating procedures, network diagrams, and configuration management documentation, if available. National, Agency, and organizational-level security instructions and policies should also be reviewed.

C3.4.1.3. Prerequisite Tasks. None.

C3.4.1.4. Input. Business Case, Mission Needs Statement, System Specifications, Architecture and Design Documents, User Manuals, Operating Procedures, Network Diagrams, Configuration Management Documents, Threat Analysis, and Federal and Agency or Service IA and security instructions and policies.

C3.4.1.5. Output/Products. None.

C3.4.2. Task 1-2, Prepare the System and Functional Description and System Identification.

C3.4.2.1. Task Objective. The objective of this task is to prepare an accurate description of the system.

C3.4.2.2. Task Description. The system and functional description and system identification task describes the system mission and functions, system capabilities and Concept of Operations (CONOPS). While the details of the system may not be clear at the outset of system development, the mission needs should provide a starting point. From the information obtained, the system's general concept and boundaries should be fairly well understood. In either developing or obtaining the system description, knowing what is not part of the system is as important as knowing what is part of the system.

C3.4.2.2.1. System Identification. Identify the system being developed or entering the C&A process. Provide the name, organization, and location of the organization developing the mission needs and the organizations containing the ultimate user.

C3.4.2.2.2. System Description. Describe the system focusing on the information security relevant features of the system. Describe all the components of the system. The system description should clearly state the purpose of the system and the capabilities desired. The system description should include a high-level description of the system architecture, including diagrams or drawings to amplify the description.

C3.4.2.2.3. Functional Description and Capabilities. Describe the system clearly delineating what functions or capabilities are expected in the fully accredited system. If the information is insufficient for the functional description to be written, the system is not ready to begin the C&A process. The functional description should include the following sections:

C3.4.2.2.3.1. System Capabilities. Clearly define the functions or capabilities expected in the fully accredited system and the mission for which it will be used. Include functional diagrams of the system. Provide the intended flows of data into the system, data manipulation, and product output.

C3.4.2.2.3.2. System Criticality. Define the system criticality and the acceptable risk[7] for the system in meeting the mission responsibilities. System criticality should consider the impact if the system were not operational (the impact of loss of life from system failure, inability to meet contingencies, impact to credibility, and danger to national security). System criticality will affect the level of risk that is acceptable. The gain realized by fielding a system with a higher security risk must exceed the risks of either not fielding or delaying fielding to implement further security measures.

C3.4.2.2.3.3. Classification and Sensitivity of Data. Define the type and sensitivity of the data processed by the system. Determine the national security classification of information to be processed (unclassified, confidential, secret and top secret) along with any special compartment. Special handling requirements must also be identified. Systems processing sensitive but unclassified information will also have additional security requirements. Identify the type of information processed (Privacy Act, financial, critical operational, proprietary, and administrative).

C3.4.2.2.3.4. System Users. Define the user's security clearances, their access rights to specific categories of information processed, and the actual information that the system is required to process. For example, a system's authorized users may include both Government and contractor personnel. If the information types indicate that proprietary information from commercial organizations other than the users will be processed, sufficient controls must be designed into the system to prevent the contractor personnel from gaining intentional or unintentional access to the proprietary data.

C3.4.2.2.3.5. System Life Cycle. Define the system life cycle and where the system is in relationship to its life cycle. [8] The expected system life-cycle information may not be known; however, there are usually significant indicators as to

---

[7] While each Service or Agency has created their own definition of acceptable risk, the generally accepted use of the term is the "Judicious and carefully considered assessment by the DAA that the residual risk inherent in the operation of the IS or network is acceptable."

[8] Although the DITSCAP is designed to be tailored to the system life cycle, it should be started as early as possible in the life cycle.

which life-cycle program is necessary to satisfy the requirement in a timely manner. For example, if a sensor support system is urgently needed to provide tactical support to ongoing operations, there is a good possibility that an accelerated development and acquisition process will be used. The C&A process must be prepared to keep pace with this effort, which requires resource allocation on the part of the Certifier and DAA.

C3.4.2.2.4. System CONOPS. Describe the system CONOPS, including functions performed jointly with other systems. Many systems have a document that describes the system CONOPS. If so include a short summary in the SSAA. The CONOPS document may be added as an appendix or listed as a reference. If a CONOPS is not available, a CONOPS must be prepared using the assistance of any existing materials and the Agencies involved.

C3.4.2.3. Prerequisite Tasks. None.

C3.4.2.4. Input. Business Case, Mission Needs Statement, System Specifications, Architecture and Design Documents, User Manuals, Operating Procedures, Network Diagrams, Configuration Management Documents, Threat Analysis, and Federal and Agency or Service IA and security instructions and policies.

C3.4.2.5. Output/Products. SSAA, Section 1.

C3.4.3. Task 1-3, Register the System.

C3.4.3.1. Task Objective. The objective of this task is to identify the Agencies and individuals involved in the C&A process and determine the current status of the system.

C3.4.3.2. Task Description. This task identifies the applicable security and user authorities and informs them of the system status.

C3.4.3.2.1. Identify Authorities. Identify the Agency or organization that will serve as the DAA, Certifier, and user representative. Identify individuals and their responsibilities in the C&A process. Each individual plays a specific and important role in the development, modification, acquisition, and use of a system. Each Agency or organization is responsible for informing the appropriate authorities when changes to an existing system are planned.

C3.4.3.3. Prerequisite Tasks. Tasks 1-1 and 1-2.

C3.4.3.4. Input. System and Functional Descriptions.

C3.4.3.5. Output/Products. None.

C3.4.4. Task 1-4, Prepare the Environment and Threat Description.

C3.4.4.1. Task Objective. The objective of this task is to define the system environment and potential threats to the system.

C3.4.4.2. Task Description. The environment and threat description task describes the operating environment, system development environment, and potential system threats. The description of the operating environment should address all relevant parts of the system's environment, including descriptions of the physical, administrative, development, and technical areas. The description should also include any known or suspected threats specifically directed at the described environment.

C3.4.4.2.1. Operating Environment. Describe the physical, personnel, communications, emanations, hardware, software, and procedural security features that will be necessary to support site operations. Operating environment security involves the measures designed to prevent unauthorized personnel from gaining physical access to equipment, facilities, material and documents and to safeguard the assets against espionage, sabotage, damage, and theft.

C3.4.4.2.1.1. Facility. Describe the physical environment in which the system will operate including floor plans, equipment placement, electrical and plumbing outlets, telephone outlets, air conditioning vents, sprinkler systems, fences, and extension of walls from true floor to true ceiling.

C3.4.4.2.1.2. Physical Security. Identify the procedures needed to counter potential threats that may come from inside or outside the organization. Identify the routine office security practices that ensure unauthorized access to protected resources is prohibited. The physical security description should also consider safety procedures for personnel operating the equipment.

C3.4.4.2.1.3. Administrative Security. Identify the administrative security procedures including the manual operations that counter threats. For example, separation of duties is an administrative activity that provides internal controls designed to make fraud, abuse, or espionage difficult without collusion.

C3.4.4.1.2.4. Personnel. Identify the number and type of personnel required to maintain the system.

C3.4.4.1.2.5. COMSEC. Determine if National Security Agency (NSA)-approved COMSEC and COMSEC key management procedures are required.

C3.4.4.1.2.6. TEMPEST. Determine if the equipment and site are required to meet TEMPEST and RED-BLACK requirements.

C3.4.4.2.1.7. Maintenance. Identify routine preventive maintenance procedures and the number of personnel required to maintain the system. Certain categories of information mandate special maintenance procedures to ensure physical security protection against unauthorized access to the information or system resources.

C3.4.4.2.1.8. Training. Identify the training for individuals associated with the system's operation and determine if the training is appropriate to their level and area of responsibility. This training should provide information about the security policy governing the information being processed as well as potential threats and the nature of the appropriate countermeasures.

C3.4.4.2.2. System Development, Integration, and Maintenance Environment. Describe the system development approach and the environment within which the system will be developed. The system development approach is an information security strategy that incorporates security into each phase of a system's life cycle. Determine where a system is in its life cycle and evaluate the status of existing documentation, development/implementation schedule, milestones, and costs. The program manager can take actions to interject the required degree of security effectively into the appropriate phases of the system's life cycle.

C3.4.4.2.2.1. Describe the information access and configuration control issues for the system. A closed security environment occurs when both of the conditions described in Table C3.T5. are true. An open security environment is any environment that does not fully meet the conditions for a closed environment.

Table C3.T5. Closed Security Environment Conditions

Security Clearance and Information Access
Software developers (including maintenance) and system integrators have sufficient clearances and authorizations to provide a reasonable level of assurance that they will not deliberately introduce malicious logic into either the environment or the system. The clearance requirements do not apply if no association or connection can be made between the development activity and the intended operational system. Sufficient clearance is defined as follows: If the maximum classification of data to be processed is confidential, developers should have a confidential clearance. If the maximum classification of data to be processed is secret or higher, developers must have at least a secret clearance. If the system will process only unclassified information, developers do not require a security clearance. However, if the system development or integration requires access to unclassified information with special controls, these individuals must first be authorized access to that information and then must abide by the special control requirements.
Configuration Control
The configuration control mechanisms must provide sufficient assurance that changes to the system are carefully controlled and introduced only after significant review and acceptance by a Configuration Control Board. The Configuration Control Board's review must include an evaluation of the impact of the proposed change on the overall system security posture. In the deliberations, the security engineer or IT security manager for the project must be an integral member of the review board.

C3.4.4.2.3. Threat Description and Risk Assessment. Define the potential threats and single points of failure that can affect the confidentiality, integrity, and availability of the system. Clearly state the nature of the threat that is expected and where possible, the expected frequency of occurrence. Unintentional human error, system design weaknesses, and intentional actions on the part of authorized as well as unauthorized users can cause these events. Most systems have common threats, such as penetration attempts by hackers, damage or misuse by disgruntled or dishonest employees, and misuse by careless or inadequately trained employees. Generic threat information is available, [9] but it must be adapted to clearly state the threats expected to be encountered by the system (perceived threat).

C3.4.4.2.3.1. Evaluate the degree of risk to the system. The cost benefit analysis of alternative is then used to identify appropriate cost-effective countermeasures to mitigate the risk. These countermeasures include technical, physical, personnel, and administrative countermeasures.

---

9 The National Security Telecommunications and Information Systems Security Committee (NSTISSIC) prepares the "Annual Assessments of the Status of National Security Telecommunications and Information Systems Security within the United States Government" that includes generic threat statements that may be tailored to the specific system. The intelligence organization that is responsible for supporting the organizations that will operate the system may also have a threat statement. There is also a sample threat statement available on the IASE.

C3.4.4.3. Prerequisite Tasks. Tasks 1-2 and 1-3.

C3.4.4.4. Input. Business Case, Mission Needs Statement, System Specifications, Architecture and Design Documents, User Manuals, Operating Procedures, Network Diagrams, Configuration Management Documents, Threat Analysis, and Federal and Agency or Service IA and security instructions and policies.

C3.4.4.5. Output/Products. SSAA, Section 2.

C3.4.5. Task 1-5, Determine the System Security Requirements.

C3.4.5.1. Task Objective. The objective of this task is to identify the system security requirements.

C3.4.5.2. Task Description. The system security requirements task defines the National, DoD and data security requirements, governing security requisites, network connection rules, and configuration management requirements. The DAA, Certifier, program manager, and user representative must reach an agreement on the security for the system and certification level based on these requirements and the CRR. The requirements may have significant cost and schedule impacts that need to be resolved in the negotiation activity.

C3.4.5.2.1. Applicable Instructions or Directives. Determine the security instructions or directives applicable to the system. In most cases, this will include national level directives, OMB Circulars A-123 (reference (l)) and A-130 (reference (d)), and DoD Directives. Each Service or Agency may also have directives that dictate security requirements. All the directives that will impact the ultimate user should be identified. The general knowledge portion of the IASE has a list of these directives and may contain the current directive or instructions or how to locate the them. Many systems are required to meet the requirements of the Trusted Computer Security Evaluation Criteria (TCSEC) (reference (m)). In these cases, the certification team should obtain the requirements for that level, for example, Level C2.

C3.4.5.2.2. Governing Security Requisites. Determine requirements stipulated by local agencies and the DAA. Contact the DAA and user representative to determine if they have any additional security requirements.

C3.4.5.2.3. Data Security Requirements. Determine the type of data processed by the system. The type of data may require additional protections. Contact the data owner or organizations that have access to the system or share data with the system to determine their security requirements.

C3.4.5.2.4. Security Concept of Operations. Describe the security CONOPS including system input, system processing, final outputs, security controls and interactions and connections with external systems. Include diagrams, maps, pictures, and tables in the security CONOPS. This section must be understandable by nontechnical managers. If a system CONOPS is available, a summary of the security portions of that CONOPS should be reviewed and added to the SSAA. If a security CONOPS, Trusted Facility Manual (TFM), or Security Features User's Guide (SFUG) is available, a summary of that information should added to the SSAA. The security CONOPS, TFM, or SFUG document may then be added as an appendix or listed as a reference in the SSAA.

C3.4.5.2.5. Network Connection Rules. Identify any additional requirements incurred if the system is to be connected to any other network or system. For example, the DISA DAA for SIPRNet has connection requirements for all systems connected to the SIPRNet. These additional security requirements must be evaluated in the C&A. These requirements and those of other systems that may be connected to the system or network must be added to the SSAA.

C3.4.5.2.6. Configuration Management. Determine if there are any additional requirements based on the Configuration Management Plan. The user representative or program manager's organization may have regulations or instructions regarding the procedures for review and approval of modifications or changes to the system. These instructions may be described in a Configuration Management Policy or Configuration Management Review Board or Change Control Board charter. These documents should be reviewed to determine if any additional requirements exist.

C3.4.5.2.7. Reaccreditation Requirements. Determine if there are unique organizational requirements related to the reaccredidation or reaffirmation of the approval to operate the system. These requirements must be documented in the SSAA.

C3.4.5.2.8. Requirements Traceability Matrix (RTM). Analyze the directives and security requisites to determine the system security requirements. Take a section of a directive and parse it into a basic security requirement statement. The security requirements may then be entered into a RTM to support the remainder of the C&A effort. Table C3.T7. provides an example of a portion of a RTM matrix. (The review column identifies the review process for each requirement, where I - Interview, D - Document Review, T - Test, and O - Observation.)

Table C3.T7. Sample RTM Format

Req. #	Requirement	Source	Related Requirement	Review				Comments
				I	D	T	O	
	1.0 GENERAL							
	1.1 FUNDAMENTAL COMPUTER SECURITY REQUIREMENTS							
FUND.1	Requirement 1 - SECURITY POLICY - There must be an explicit and well-defined security policy enforced by the system.....	TCSEC INTRO. p.3, TNI 2.2.1	DOJ 2640.2C - 14	X	X	X		See FUND.2 - FUND.6
FUND.2	Requirement 2 - MARKING - Access control labels must be associated with objects....	TCSEC INTRO. p.3	TCSEC 2.2.1.1	X	X	X		See DAC.1 - DAC.6
	1.2 GENERAL REQUIREMENTS							
GEN.1	Agencies must implement and maintain a program to assure that adequate security (see definition in App. A) is provided for all Agency information collected, processed, transmitted, stored, or disseminated in general support systems & major applications.	OMB Circ. A-130 Appendix III, A. 3.(reference (d))		X	X		X	

C3.4.5.3. Prerequisite Tasks. Tasks 1-2 through 1-4.

C3.4.5.4. Input. National Directives, OMB Circulars, DoD Directives, Service or Agency directives, as applicable, System CONOPS, Security CONOPS, Trusted Facility Manual, Security Features Users Guide, Configuration Management Documents.

C3.4.5.5. Output/Products. SSAA, Section 5.

C3.4.6. Task 1-6, Prepare the System Architecture Description.

C3.4.6.1. Task Objective. The objective of this task is to prepare a high level overview of the types of hardware, software, firmware and associated interfaces envisioned for the completed system. Refinements and changes to the architecture should be made after completing the system security requirements and as the SSAA is reviewed and revised.

C3.4.6.2. Task Description. The system architecture task defines the system hardware, software, firmware, and interfaces. This description contains an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communications processors, network, and remote interfaces. The system architecture includes the configuration of any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information and includes computers, ancillary equipment, software, firmware, and similar procedures and services, including support services and related resources.

C3.4.6.2.1. System Hardware. Describe the target hardware and its function. Include an equipment list as an attachment. If the development effort involves a change of existing hardware, identify the specific hardware components being changed.

C3.4.6.2.2. System Software. Describe the operating system(s), database management system(s), and software applications and how they will be used. Identify whether the software is commercial off-the-shelf (COTS), Government off-the-shelf (GOTS), or on the Evaluated Product List (EPL). This includes manufacturer-supplied software, other COTS, and all program-generated application software.

C3.4.6.2.3. System Firmware. Describe the firmware that is stored permanently in a hardware device that allows reading and executing of the software, but not writing or modifying it. For example, firmware includes programmable read-only memory (PROM) and enhanced PROM (EPROM) devices. State whether the firmware is a standard commercial product, unique, or on the EPL.

C3.4.6.2.4. System Interfaces. Describe the system's external interfaces including the purpose of each external interface and the relationship between the interface and the system. Describe the significant features of the communications

layout, including a high level diagram of the communications links and encryption techniques connecting the components of the system, associated data communications, and networks.

C3.4.6.2.5. Data Flows. Describe the system's internal interfaces and data flows including the types of data and the general methods for data transmission. Describe the specific transmission media or interfaces to other systems. The description must include diagrams or text to explain the flow of critical information from one component to another.

C3.4.6.2.6. Accreditation Boundary. Describe the boundary of the system. The description must include diagrams or text to clearly delineate which components are to be evaluated as part of the C&A task and which are not included. All components included must be described in the systems description. Elements outside the accreditation boundary must be included in the section on external interfaces.

C3.4.6.3. Prerequisite Tasks. Tasks 1-1 through 1-5.

C3.4.6.4. Input. System Specification, Architecture and Design Documents, and Network Diagrams.

C3.4.6.5. Output/Products. SSAA, Section 3.

C3.4.7. Task 1-7, Identify the C&A Organizations and the Resources Required.

C3.4.7.1. Task Objective. The objective of this task is to identify the organizations and individuals involved in the C&A process.

C3.4.7.2. Task Description. This task identifies the appropriate authorities, resource, and training requirements and determines the certification team's roles and responsibilities. The C&A process may involve many organizations spanning a number of roles.

C3.4.7.2.1. Organizations. Identify the organizations, individuals, and titles of the key authorities in the C&A process.

C3.4.7.2.2. Resources. Identify the resources required to conduct the C&A. If a contractor is involved or individuals from other Government organizations are temporarily detailed to assist in the C&A process, funding requirements must be defined and included in the SSAA. The composition and size of the team will depend

of the size and complexity of the system. The team must have members with composite expertise in the whole span of activities requirement and who are independent of the system developer or project manager. Identify the roles of the certification team and their responsibilities.

C3.4.7.2.3. Resources and Training Requirements. Describe the training requirements, types of training, who is responsible for preparing and conducting the training, what equipment is required, and what training devices must be developed to conduct the training, if training is required. Funding for the training must be identified.

C3.4.7.2.4. Other Supporting Organizations. Identify any other organizations or working groups that are supporting the C&A process.

C3.4.7.3. Prerequisite Tasks. Tasks 1-2 and 1-3.

C3.4.7.4. Input. None.

C3.4.7.5. Output/Products. SSAA, Section 6.

C3.4.8. Task 1-8, Tailor the DITSCAP and Prepare the DITSCAP Plan.

C3.4.8.1. Task Objective. The objective of this task is to tailor the DITSCAP to the system and prepare the DITSCAP plan.

C3.4.8.2. Task Description. This task determines the appropriate certification level and adjusts the DITSCAP activities to the program strategy and system life cycle. Tailoring the security activities to system development activities ensures that the security activities are relevant to the process and provide the required degree of analysis. Tailoring permits the DITSCAP to remain responsive to operational requirements and priorities.

C3.4.8.2.1. Certification Level. Determine the certification level. While the C&A phases and activities remain the same for any system, the level of analysis is tailored to the system. Four levels of certification are identified in Table C3.T8.

Table C3.T8. Certification Levels

Level	Certification Level	Description
1	Minimum Security Checklist	Level 1 requires completion of the minimum security checklist. The system user or an independent Certifier may complete the checklist.
2	Minimum Analysis	Level 2 requires the completion of the minimum security checklist and independent certification analysis.
3	Detailed Analysis	Level 2 requires the completion of the minimum security checklist and a more in-depth, independent analysis.
4	Extensive Analysis	Level 4 requires the completion of the minimal security checklist and the most extensive independent analysis.

C3.4.8.2.1.1. Select the alternative for each of the seven characteristics that describe the system. The alternatives are described in the following sections. Each system characteristic selection has an assigned weight. Enter the assigned weight in the right column on Table C3.T9. The total of these weights is used to select the appropriate certification level.

Table C3.T9. System Characteristics an Weights

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

C3.4.8.2.1.1.1. Interfacing Mode. The interfacing mode categorizes interaction. The question concerns containment of risk; for example, if a problem were to occur with the operation, data, or system, what would be the risk to other operations, data, or systems with which it interacts. The interactions of systems may be through either physical or logical relationships. These relationships are referred to as benign, passive, or active.

C3.4.8.2.1.1.1.1. Benign. A benign system has no interaction with other systems (no physical or logical relationships). All relationships are restricted to a closed community.

C3.4.8.2.1.1.1.2. Passive. In a passive system, the system has only indirect interaction with other systems; systems may or may not have physical relationships, but have tightly controlled logical relationships. An example of a passive system is receive only, no interactive sessions. The passive case permits lower-level protocols to support passive interactions.

C3.4.8.2.1.1.1.3. Active. An active system has direct interaction with other systems, with both physical and logical relationships. The active case may allow multiple interactive sessions with multiple operations, systems, infrastructures, or data.

C3.4.8.2.1.1.2. Processing Mode. The processing mode distinguishes the way processing, transmission, storage, or data is handled. It reflects the use of the system by one or more different sets of users or processes. The alternatives are dedicated mode, compartmented mode, system high, and multilevel. Each of the modes exhibits unique security qualities.

C3.4.8.2.1.1.2.1. Dedicated Mode. Dedicated mode is where each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has a valid security clearance for all the information within the system, formal access approval, and signed nondisclosure agreements for all the information stored and/or processed by the system. The user also has a valid need-to-know for all the information contained within the IS. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

C3.4.8.2.1.1.2.2. System High Mode. System High mode is where each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has a valid security clearance for all the information within the IS, formal access approval, and signed nondisclosure agreements for all the information stored and/or processed by the system. The user also has a valid need-to-know for some of the information contained within the IS.

C3.4.8.2.1.1.2.3. Compartmented Mode. Compartmented mode is where each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has a valid security clearance for the most restricted information processed in the system, formal access approval, and signed nondisclosure agreements for the information that a user is to have access. The user also has a valid need-to-know for the information to which they have access.

C3.4.8.2.1.1.2.4. Multilevel Mode. Multilevel mode is where some of the users, with direct or indirect access to the system, its peripherals, remote, terminals, or remote hosts, do not have a valid security clearance for all the information processed in the IS. All users have the proper security clearance, formal access approval, and a valid need-to-know for that information to which they have access.

C3.4.8.2.1.1.3. Attribution Mode. The attribution mode distinguishes the degree or complexity of accountability required to identify, verify, and trace system entities as well as changes in their status. The four alternatives are none, rudimentary, selected, and comprehensive.

C3.4.8.2.1.1.3.1. None. None means no processing, transmission, storage, or data carries the need to attribute them to users or processes.

C3.4.8.2.1.1.3.2. Rudimentary. Rudimentary means the most basic processing, transmission, storage, or data carries the need to attribute them to users or processes.

C3.4.8.2.1.1.3.3. Selected. Selected means some processing, transmission, storage, or data carries the need to attribute them to users or processes.

C3.4.8.2.1.1.3.4. Comprehensive. Comprehensive means all or almost all processing, transmission, storage, or data carries the need to attribute them to users or processes.

C3.4.8.2.1.1.4. Mission-Reliance. Mission-reliance relates the degree to which the success of the mission relies on the operation, data, infrastructure, or system. The criticality of the mission in a broader context is independent of that factor and is used separately. The four alternatives are none, cursory, partial, or total.

C3.4.8.2.1.1.4.1. None. None means that the mission is not dependent on the specific aspect (the operation, data, infrastructure, or system).

C3.4.8.2.1.1.4.2. Cursory. Cursory means that the mission is only indirectly dependent on the specific aspect (the operation, data, infrastructure, or system).

C3.4.8.2.1.1.4.3. Partial. Partial means that the mission is partially dependent on the specific aspect (the operation, data, infrastructure, or system).

C3.4.8.2.1.1.4.4. Total. Total means that the mission is totally dependent on the specific aspect (the operation, data, infrastructure, or system).

C3.4.8.2.1.1.5. Availability. Availability relates the degree to which the operation, data, infrastructure, or system needs to be available from a security perspective. Availability concerns are those that relate to security risks (non-tolerable operational impacts) and does not include those that are only performance concerns. The four alternatives are reasonable, soon, As Soon As Possible (ASAP), or immediate.

C3.4.8.2.1.1.5.1. Reasonable. Reasonable means that the specific aspect (the operation, data, infrastructure, or system) must be available in reasonable time to avoid operational impacts.

C3.4.8.2.1.1.5.2. Soon. Soon means that the specific aspect (the operation, data, infrastructure, or system) must be available soon (timely response) to avoid operational impacts.

C3.4.8.2.1.1.5.3. As Soon As Possible ASAP). ASAP means that the specific aspect (the operation, data, infrastructure, or system) must be available as soon as possible (quick response) to avoid operational impacts.

C3.4.8.2.1.1.5.4. Immediate. Immediate means that the specific aspect (the operation, data, infrastructure, or system) must be available immediately (on demand) to avoid operational impacts.

C3.4.8.2.1.1.6. Integrity. Integrity relates the degree to which the integrity of operation, data, infrastructure, or system is needed from a security perspective. Integrity concerns are those that relate to security risks (non-tolerable operational impacts) and does not include those that are only performance concerns. The three alternatives are not-applicable, approximate, or exact.

C3.4.8.2.1.1.6.1. Not-Applicable. Not-applicable means that the degree of integrity for a specific aspect (the operation, data, infrastructure, or system) is irrelevant as to operational impacts.

C3.4.8.2.1.1.6.2. Approximate. Approximate means that the degree of integrity for a specific aspect (the operation, data, infrastructure, or system) must be approximate in order to avoid operational impacts.

C3.4.8.2.1.1.6.3. Exact. Exact means that the degree of integrity for a specific aspect (the operation, data, infrastructure, or system) must be exact in order to avoid operational impacts.

C3.4.8.2.1.1.7. Information Category. The mission of each system will determine the information that is processed. The mission and information will influence the environment and security requirements applicable to each information category. Information categories are defined by their relationships with common management principles and security requirements promulgated by the security policy for each information category. Processing, transmission, storage, and data of more than one category of information does not create a new category but instead inherits and must satisfy all the security requirements of the assigned categories. Each of the identified categories may carry additional restrictions or special handling conditions such as NATO-releasable or No Foreign Dissemination (NOFORN). The information categories are unclassified, sensitive, confidential, secret, top secret, or compartmented and/or special access classified.

C3.4.8.2.1.1.7.1. Unclassified. This category of information includes all information that is not classified and is not sensitive as defined below.

C3.4.8.2.1.1.7.2. Sensitive Information. This category includes information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interests or the conduct of Federal programs, or the privacy that individuals are entitled under 5 U.S.C. Section 552a (reference (at)), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Systems that are not national security systems, but contain sensitive information are to be protected according to the requirements of P.L. 100-235 (reference (c)). In many cases, it may be useful to further characterize the sensitive information by determining the subcategory. This may indicate additional national, DoD, Service, or Agency requirements that are imposed by processing that type of information. The subcategories are:

C3.4.8.2.1.1.7.2.1. Privacy Act. This category includes all information covered by the Privacy Act, including medical, pay, and personnel

information. Information may be either classified or unclassified. Privacy Act category information requires handling according to a common sensitivity. Privacy Act information usually requires system and information access control.

C3.4.8.2.1.1.7.2.2. Financially Sensitive. This category includes financially and contractually sensitive information. Information may be either classified or unclassified. Financially sensitive category information usually requires handling according to a common sensitivity, but may require special assurance mechanisms such as two-person verification of transactions. Financially sensitive category information requires system and information access control.

C3.4.8.2.1.1.7.2.3. Proprietary. This category includes information provided by a source or sources under the condition that it not be released to other sources. This information may require system or information access control.

C3.4.8.2.1.1.7.2.4. Administrative/Other. This category includes DoD information associated with housekeeping activities, information marked For Official Use Only, and unclassified information that does not fall into any of the other information categories.

C3.4.8.2.1.1.7.3. Confidential. This category includes all classified information designated Confidential. The disclosure of confidential information could reasonably be expected to cause damage to national security. A security clearance is required for access to Confidential materials and systems.

C3.4.8.2.1.1.7.4. Secret. This category includes all classified information designated Secret. The disclosure of secret information could reasonably be expected to cause serious damage to national security. A security clearance is required for access to Secret materials and systems.

C3.4.8.2.1.1.7.5. Top Secret. This category includes all classified information designated Top Secret. The disclosure of top secret information could reasonably be expected to cause exceptionally grave damage to national security. A security clearance is required for access to Top Secret materials and systems.

C3.4.8.2.1.1.7.6. Compartmented/Special Access Classified. This category includes all information that requires special access and a security clearance. Examples include Sensitive Compartmented Information (SCI), Single Integrated Operations Plan-Extremely Sensitive Information (SIOP-ESI), and special access programs.

C3.4.8.2.1.2. Based on the total weights calculated for the system, select the certification level using Table C3.T10. In some cases the characteristics of a particular category may dictate a higher classification level that that indicated by the total weights. In these cases, the higher weight should be used.

Table C3.T10. Certification Level

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

C3.4.8.2.1.3. After the system characteristic alternatives are selected and the appropriate weight entered into the chart, the total weight of the system is calculated. Using Table C3.T10., the appropriate level is identified. Table C3.T11. provides an example for determining the certification level. With a total weight of 27, the following system would be evaluated at either Level 2 or 3 as agreed to by the DAA, Certifier, program manager, or user representative.

Table C3.T11. Certification Level Example

Characteristic	Alternative	Weight
Interfacing Mode	Active	6
Processing Mode	System High	2
Attribution Mode	Basic	3
Mission-Reliance	Total	7
Availability	ASAP	4
Integrity	Approximate	3
Information Categories	Sensitive	2
Total of all weights		27

C3.4.8.2.2. Tailoring. Tailor the DITSCAP process to address the specific needs of the system, security requirements, and program requirements.

C3.4.8.2.2.1. Programmatic Considerations. Adjust the DITCAP tasks to the selected program strategy. This Manual generally describes the DITSCAP for the grand design acquisition strategy (see Chapter 7). Other program strategies may require tailoring. For example, if the system is to be built and fielded in increments, the C&A process should be adapted to evaluate the increments as they are

developed and fielded. If an increment does not modify the security-related portions of the system, then C&A activities may not be necessary for that increment. Similarly, if an increment changes only a portion of the system, then the C&A may be adapted to examine only the portions of the system that have been modified. The approach should be clearly defined in the SSAA.

C3.4.8.2.2.2. Security Environment. Identify any security requirements that might affect the level of effort required for the C&A process. The security requirements may include personnel, physical, administrative, procedural, operational, computer, network, and communications security components.

C3.4.8.2.2.3. IS Characteristics. Identify the characteristics of the system that might influence the level of effort required for the C&A process.

C3.4.8.2.4. DITSCAP Plan. Prepare a DITSCAP plan that documents the tailoring and defines the activities required for the C&A process. The tasks, milestones and schedule must be consistent with the system development or maintenance schedule. The level of effort and roles and responsibilities must also be consistent with the program development process and management plan. The DAA, Certifier, program manager, and user representative must review the SSAA and DITSCAP plan to ensure the C&A effort is consistent with the program schedules. The DAA must receive certification evidence in sufficient time to review the material and make an informed decision regarding the approval to operate the system.

C3.4.8.3. Prerequisite Tasks. Tasks 1-4 through 1-7.

C3.4.8.4. Input. None.

C3.4.8.5. Output/Products. SSAA, Section 7.

C3.4.9. Task 1-9, Draft the SSAA.

C3.4.9.1. Task Objective. The objective of this task is to complete and assemble the SSAA document.

C3.4.9.2. Task Description. This task completes the SSAA document. As each Phase 1 task is completed, a section of the SSAA is prepared. These sections must be assembled into the formal SSAA document. The certification team is responsible for the preparing the SSAA. After the document is completed, the draft SSAA is submitted to the DAA, Certifier, program manager, and user representative

for their review. The draft SSAA establishes a reference for discussions during negotiation.

C3.4.9.3. Prerequisite Tasks. Task 1-1 through Task 1-8.

C3.4.9.4. Input. Draft SSAA sections.

C3.4.9.5. Output/Products. Completed draft Phase 1 SSAA document.

C3.4.10. Task 1-10, Conduct Certification Requirements Review.

C3.4.10.1. Task Objective. The objective of this task is to conduct a CRR.

C3.4.10.2. Task Description. The CRR task provides an opportunity for the DAA, Certifier, program manager, and user representative to discuss the system functionality, security requirements, level of effort, and planned C&A scheduled. The CRR must result in an agreement regarding the level of effort and the approach that will be taken to implement the security requirements.

C3.4.10.3. Prerequisite Tasks. Task 1-1 through Task 1-9.

C3.4.10.4. Input. Completed draft Phase 1 SSAA document.

C3.4.10.5. Output/Products. None.

C3.4.11. Task 1-11 Establish Agreement on Level of Effort and Schedule.

C3.4.11.1. Task Objective. The objective of this task is to agree on the C&A level of effort and schedule.

C3.4.11.2. Task Description. This task ensures that the DAA, Certifier, program manager, and user representative agree to the level of effort and schedule for the C&A activities.

C3.4.11.3. Prerequisite Tasks. Task 1-10.

C3.4.11.4. Input. Completed draft Phase 1 SSAA document.

C3.4.11.5. Output/Products. None.

C3.4.12. Task 1-12, Approve Phase 1 SSAA.

C3.4.12.1. Task Objective. The objective of this task is to obtain the DAA's approval on the Phase 1 SSAA.

C3.4.12.2. Task Description. In this task the DAA makes a decision on the Phase 1 SSAA, approving the system functionality, operating environment, development environment, potential threats, security requirements, system architecture, organization and resource requirements, tailoring factors, certification level, and DITSCAP plan.

C3.4.12.3. Prerequisite Tasks. Task 1-11.

C3.4.12.4. Input. SSAA.

C3.4.12.5. Output/Products. Approved SSAA.

C3.5. PHASE 1 ROLES AND RESPONSIBILITIES

C3.5.1. Security Roles and Responsibilities.

C3.5.1.1. DAA Responsibilities. The DAA must continuously review the system for compliance with the SSAA. During the C&A, the Certifier, and certification team support the DAA. At other times, the DAA will be supported by the system Information Systems Security Officer (ISSO). The level and type of support will be defined by the organizations involved. During Phase 1, the DAA is responsible for the activities shown in Table C3.T12.

Table C3.T12. DAA Responsibilities

1.	Define accreditation requirements.
2.	Obtain a threat assessment for the system.
3.	Assign a Certifier to conduct vulnerability and risk assessments.
4.	Support the DITSCAP tailoring and level of effort determination.
5.	Approve the SSAA.

C3.5.1.2. Certifier and Certification Team Responsibilities. During Phase 1, the Certifier and certification team are responsible for the activities shown in Table C3.T13.

Table C3.T13. Certifier and Certification Team Responsibilities

1.	Support the DAA as the technical expert in the certification process.
2.	Begin vulnerability and risk assessments.
3.	Review threat definition.
4.	Identify the security requirements.
5.	Tailor the DITSCAP, determine the appropriate certification level, and prepare the DITSCAP Plan.
6.	Provide level of effort and resource requirements.
7.	Develop the SSAA.
8.	Provide oversight for the CRR.

C3.5.1.3. ISSO Responsibilities. During Phase 1, the ISSO is responsible for the duties shown in Table C3.T14.

Table C3.T14. ISSO Responsibilities

1.	Assist the DAA, Certifier, and certification team in the certification effort.
2.	Review the business case or mission statement to determine that it accurately describes the system.
3.	Review the environment description to verify that it accurately describes the system.

C3.5.2. User Representative Responsibilities. The user representative provides input into the SSAA to ensure that the system meets the operational need, will meet availability and integrity requirements, and has a realistic security policy that can be maintained in the operational environment. During Phase 1, the user representative is responsible for the duties shown in Table C3.T15.

Table C3.T15. User Representative Responsibilities

1.	Support the DITSCAP tailoring and level of effort determination.
2.	Provide a business case or mission statement.
3.	Validate or define system performance, availability, and functionality requirements.
4.	Provide data sensitivity, end user functionality, and user organization information.
5.	Verify the ability to comply with the SSAA during operations.

C3.5.3. Acquisition or Maintenance Organization Responsibilities.

C3.5.3.1. Program Manager Responsibilities. During Phase 1, the program manager is responsible for system development and supports the security process. The program manager's responsibilities in Phase 1 are shown in Table C3.T16.

Table C3.T16. PM Responsibilities

1.	Initiate the dialogue with the DAA, Certifier, and user representative.
2.	Define the system schedule and budget.
3.	Support the DITSCAP tailoring and determine the certification level.
4.	Define the system architecture.
5.	Integrate system security requirements into the system.
6.	Prepare Life-Cycle Management Plans.
7.	Define the security architecture.

C3.5.3.2. Program Management Support Staff Responsibilities. During Phase 1, the program management support staff provides support to the program manager to determine the level of effort and provide cost and schedule evaluations.

C3.5.3.3. Developer, Integrator, or Maintainer Responsibilities. During Phase 1, the developer, integrator, or maintainer is responsible for the duties shown in Table C3.T17.

Table C3.T17. Developer, Integrator or Maintainer Responsibilities

1.	Provide technical equipment environment requirements.
2.	Provide target hardware and software architecture.
3.	Provide information regarding the system development organization.
4.	Determine the feasibility of technical solutions and security requirements.

C3.5.3.4. Configuration Management Responsibilities. During Phase 1, the configuration management staff support the program manager in the development and maintenance of system and system documentation.

C3.5.3.5. System Administration Responsibilities. There are no system administration responsibilities in Phase 1.

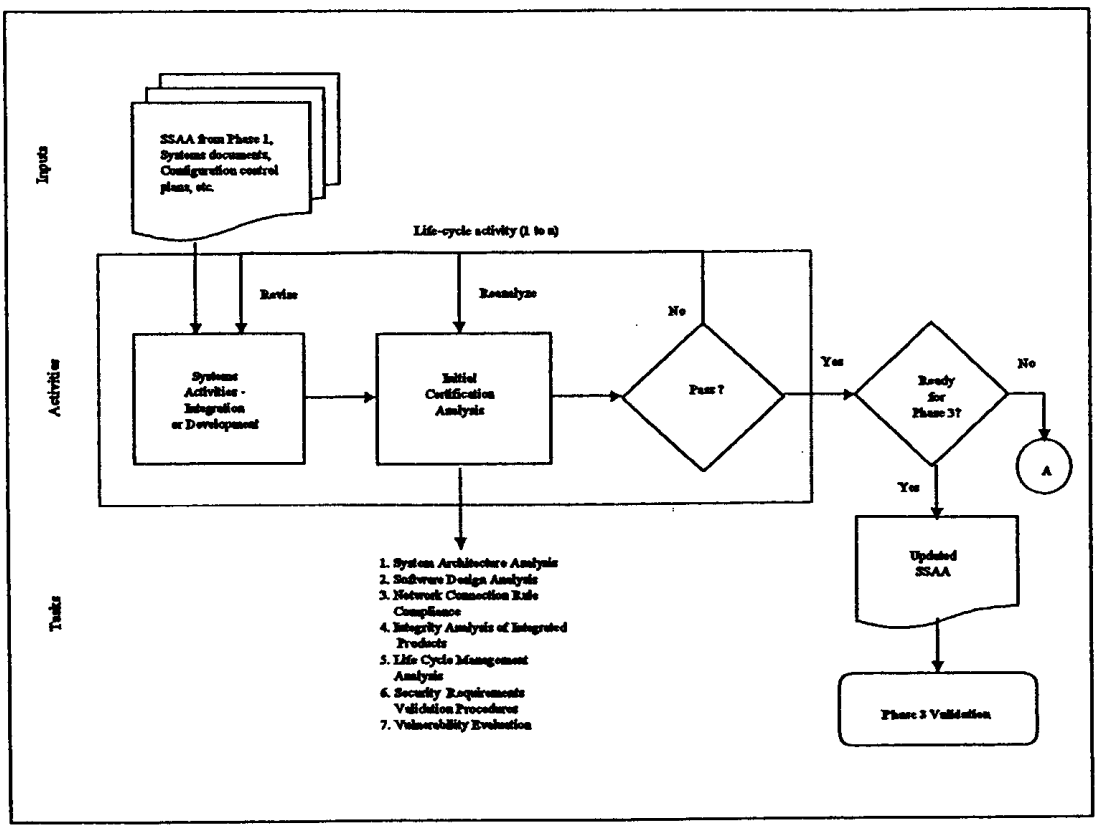
C4. CHAPTER 4

PHASE 2, VERIFICATION

C4.1. PHASE 2 OVERVIEW

C4.1.1. Phase 2 activities, Figure C4.F1., verify the evolving system's compliance with the risk management requirements in the SSAA. These activities occur between the signing of the initial version of the SSAA and the certification of the system or components (beginning of Phase 3). Phase 2 activities include verifying security requirements during system development or modification, certification analysis, CT&E (type accreditation only), and analysis of the certification results. The SSAA is refined during Phase 2.

Figure C4.F1. Verification Activities



C4.1.2. Phase 2 starts with a review of the SSAA and ends with an updated SSAA for Phase 3. Phase 2 activities examine the evolving system in a process similar to an

Independent Verification and Validation (IV&V). As the system development activity progresses and details of the system evolve, the certification effort examines the updated system and its design. All the Phase 2 activities are tailored to meet the certification level defined in Phase 1.

C4.2. PHASE 2 ACTIVITIES

C4.2.1. SSAA Refinement. Phase 2 starts with a review of the SSAA. If there has been a significant time delay since the completion of Phase 1 or if new people are involved in the C&A process, the SSAA should be reviewed in detail. The SSAA is updated throughout Phase 2 to include changes made during system development or modification and to include the results of the certification analysis. At each stage of the development or modification, details are added to the SSAA. Any changes in the system that affect its security posture must be submitted to the DAA, Certifier, program manager, and user representative for approval and inclusion in the revised SSAA.

C4.2.1.1. During the Phase 2 activities, evidence is collected to support the certification. As more details about the hardware and software architecture become available, the design information is added to the SSAA as justification to support the agreed on level of certification actions. When security test plans and procedures are completed they are added to the SSAA. Security testing resource estimates should be reviewed and refined as system development or modification continues. This information must also be included in the SSAA. Vulnerability Evaluation Reports and Analysis Summary Reports are included with the evidence and added to the SSAA. Should any changes occur to the security posture proposed in the approved SSAA, these changes need to be submitted to the DAA, Certifier, program manager, and user representative for approval and inclusion in the revised agreement.

C4.2.2. System Development and Integration. System development and integration activities are those activities required for development or integration of the IS components as defined in the system's functional and security requirements. The specific activities will vary depending on the overall program strategy, the life-cycle management process, and the position of the IS in the life cycle. During system development and integration, there are corresponding Phase 2 certification analysis tasks. This activity verifies that the requirements in the SSAA are met in the evolving system before it is integrated into the operating environment.

C4.2.3. Initial Certification Analysis. The initial certification analysis determines if the IS is ready to be evaluated and tested during Phase 3, Validation.

Initial certification analysis verifies that the development, modification, and integration efforts will result in a higher probability of success for an accreditable IS before Phase 3 begins. Certification tasks are tailored to the system development activities to ensure that the tasks are relevant to the process and provide the required degree of analysis to ensure conformance with the SSAA. Tailoring also gives the DITSCAP the flexibility to adjust the level of effort to fit the operational need. In that manner, tailoring permits the DITSCAP to remain responsive to national and military priorities.

C4.2.3.1. The initial certification analysis verifies by analysis, investigation, and comparison methodologies that the IS design implements the SSAA requirements and that the IS components that are critical to security, function properly. Phase 2 initial analysis tasks complement the functional testing certification tasks that occur during Phase 3. Each of these tasks is discussed in greater detail in the following sections. Phase 2 tasks are identified in Table C4.T1.

Table C4.T1. Initial Certification Tasks During Verification

1.	System Architecture Analysis.
2.	Software Design Analysis.
3.	Network Connection Rule Compliance Analysis.
4.	Integrity Analysis of Integrated Products.
5.	Life-Cycle Management Analysis.
6.	Security Requirements Validation Procedures Preparation.
7.	Vulnerability Assessment.

C4.2.3.2. When the Phase 2 initial certification analysis is completed the system should have a documented security specification, comprehensive test plan and procedures, and written assurance that all network and other interconnection requirements have been determined. When systems are being deployed to multiple locations, their planned interfaces with other components of the operating environment must be verified. COTS and GOTS products used in the system design must be evaluated to ensure that they have been integrated properly and that their functionality meets the security and operational needs of the system. Life-cycle management plans must be analyzed to verify that sufficient plans and procedures are in place to maintain the security posture. Phase 3 test procedures are prepared as applicable. Phase 2 tasks conclude with a vulnerability assessment to identify the risk that must be addressed by physical, personnel, procedural, or educational training and awareness in the operational environment.

C4.2.4. Assess Analysis Results. At the conclusion of each development or

integration milestone, the certification analysis results are reviewed. If the results indicate significant deviation from the SSAA, the DITSCAP should return to Phase 1 to resolve the problems. If the results are acceptable, the DITSCAP proceeds to the next task or to Phase 3.

C4.3. INITIAL CERTIFICATION ANALYSIS TASKS

C.4.3.1. The certification analysis tasks are discussed in the sections below. After each task is completed, a Task Analysis Summary Report must be prepared. This report must include the information shown in Table C4.T2. Complete the Minimum Security Activity Checklist, Appendix 2, for each task and level. The Minimum Security Checklist is exempt from licensing in accordance with paragraph C4.4.3. of DoD 8910.1-M (reference (au)).

Table C4.T2. Task Analysis Summary Report Topics

1.	Record of findings.
2.	Evaluation of vulnerabilities discovered during evaluations.
3.	Summary of the analysis level of effort.
4.	Summary of tools used and results obtained.
5.	Recommendations.

C4.3.2. Task 2-1, System Architecture Analysis.

C4.3.2.1. Task Objective.& The objective of this task is to ensure that the system architecture complies with the architecture description agreed on in the SSAA.

C4.3.2.2. Task Description. The system architecture analysis task verifies how well the security requirements defined in the SSAA are integrated into the system security architecture. The security architecture should state clearly which requirements are to be implemented by the system architecture and which requirements will be satisfied within the system's operating environment. Analysis of system level information reveals how effectively the security architecture implements the security policy and requirements. The interfaces between this and other systems must be identified. These interfaces must be evaluated to assess their effectiveness in maintaining the security posture of the infrastructure.

C4.3.2.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C4.3.2.2.2. Level 2. Complete the Minimal Security Activity Checklist. Analyze the system level information to evaluate the security architecture

compliance with the approach stated in the SSAA. The system architecture must be evaluated for compliance with the security requirements. The interfaces between this and other systems must be identified and their ability to preserve the security integrity must be evaluated. The system architecture must be evaluated for consistency with other governing architectures (Department of Defense Intelligence Information System (DoDIIS) Reference Model, etc.).

C4.3.2.2.3. Level 3. Complete the Minimal Security Activity Checklist. Conduct a **detailed analysis** of the system level information to evaluate the security architecture compliance with the stated approach in the SSAA. The system architecture must be evaluated for compliance with the security requirements. The interfaces between this and other systems must be identified and their ability to preserve the security integrity must be evaluated. **Security test plans and procedures must be developed. Each security requirement identified in the SSAA must be validated through testing.** The system architecture must be evaluated for consistency with other governing architectures (DoDIIS Reference Model, etc.).

C4.3.2.2.4. Level 4. Complete the Minimal Security Activity Checklist. Conduct a **comprehensive analysis** of the system level information to evaluate the security architecture compliance with the stated approach in the SSAA. The system architecture must be evaluated for compliance with the security requirements. The interfaces between this and other systems must be identified and their ability to preserve the security integrity must be evaluated. **The system analysis must include fault tree analysis, flaw hypothesis, or similar types of analysis.** Security test plans and procedures must be developed. Each security requirement identified in the SSAA must be validated through testing. The system architecture must be evaluated for consistency with other governing architectures (DoDIIS Reference Model, etc.).

C4.3.2.3. Prerequisite tasks. System design.

C4.3.2.4. Input. SSAA, System Architecture, and System Design Specifications.

C4.3.2.5. Output/Products. A System Architecture Analysis Summary Report must be prepared. This report must include the items shown in Table C4.T2.

C4.3.2.6. Suggested References.

C4.3.2.6.1. "Systems Engineering Management Guide" (Defense Systems Management College, January 1990) (reference (n))

C4.3.2.6.2. "Computer Security Considerations in Federal Procurements" (NIST Special Publication 800-4) (reference (o))

C4.3.2.6.3. "Trusted Database Management System Interpretation" (NCSC-TG-012) (reference (p)).

C4.3.2.6.4. "Assessing Controlled Access Protection" (NCSC-TG-028) (reference (q)).

C4.3.2.6.5. "A Guide to Understanding Design Documentation in Trusted Systems" (NCSC-TG-021, Version 1) (reference (r))

C4.3.2.6.6. "Trusted Network Interpretation Environments Guideline" (NCSC-TG-011, Version 1) (reference (s))

C4.3.2.6.7. "A Guide to Understanding Trusted Recovery in Trusted Systems" (NCSC-TG-022, Version 1) (reference (t))

C4.3.3. Task 2-2, Software, Hardware, and Firmware Design Analysis.

C4.3.3.1. Task Objective. The objective of this task is to assess the software, hardware, and firmware security architecture to evaluate the compliance of the design with the stated approach in the SSAA and to evaluate compliance with all planned requirements.

C4.3.3.2. Task Description. This task evaluates how well the software, hardware, and firmware reflects the specified technical security requirements of the SSAA and the security architecture of the system. This task will identify and evaluate security-critical software, hardware, and firmware, and evaluate the design, and identify and evaluate the vulnerabilities. This task may include a detailed analysis of software, hardware, and firmware specifications and design documentation. The Trusted Computing Base (TCB) must be identified and analyzed for proper and full implementation of the security requirements. The task must assess whether the critical security features (identification and authentication, access controls, auditing, etc.) are implemented correctly and completely.

C4.3.3.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C4.3.3.2.2. Level 2. Complete the Minimal Security Activity Checklist. Analyze the system design, software, hardware, and firmware

specifications, and design documentation. The design must be evaluated for compliance with the approach stated in the SSAA. This evaluation must include an examination of the software, hardware, and firmware requirements specification to ensure the security requirements in the security architecture are traceable to specific requirements.

C4.3.3.2.2.1. The security-critical components of the software, hardware, and firmware and the functions they perform, must be identified. The functional performance of these components must be analyzed and evaluated to determine if the components completely and sufficiently perform the required security functions. Any discrepancies must be evaluated as potential security vulnerabilities. This examination must include software applications, software routines, operating system (O/S) features, firmware, and hardware capabilities critical to maintaining the security (confidentiality, integrity, availability, and accountability) standards necessary for certification and accreditation.

C4.3.3.2.3. Level 3. Complete the Minimal Security Activity Checklist. Conduct a **detailed analysis** of the system design, software, hardware, and firmware specifications, and design documentation. The design must be evaluated for compliance with the approach stated in the SSAA. This evaluation must include an examination of the software, hardware, and firmware requirements specification to ensure the security requirements **are in the requirements specification and are traceable to specific features in the system architecture. Review the design by analyzing design documentation and attending design reviews. The analysis must include fault tree or flaw analysis. The interfaces between components must be examined for compliance with the security requirements. The examination includes all interfaces with software previously developed (COTS, GOTS, or reuse software). The analysis and evaluation must determine if the identification and authentication, access controls, and discretionary access controls have been implemented correctly and completely.**

C4.3.3.2.3.1. The security-critical components of the software, hardware, and firmware and the functions they perform, must be identified. The functional performance of these components must be analyzed and evaluated to determine if the components completely and sufficiently perform the required security functions. Any discrepancies must be evaluated as potential security vulnerabilities. This examination must include software applications, software routines, O/S features, firmware, and hardware capabilities critical to maintaining the security (confidentiality, integrity, availability, and accountability) standards necessary for certification and accreditation.

C4.3.3.2.3.2. **If a TCB has been integrated into the system, the boundaries must be examined to ensure that they are clearly defined and that the integrity of the TCB is maintained in its interaction with other system components. The examination must determine that only external interfaces are used by non-TCB elements to access the TCB.**

C4.3.3.2.4. Level 4. Complete the Minimal Security Activity Checklist. Conduct a **comprehensive analysis** of the system design, software, hardware, and firmware specifications, and design documentation. The design must be evaluated for compliance with the approach stated in the SSAA. This evaluation must include an examination of the software, hardware, and firmware requirements specification to ensure the security requirements are in the requirements specification and are traceable to specific features in the system architecture. Review the design by analyzing design documentation and attending design reviews. The analysis must include fault tree or flaw analysis, **and if appropriate, covert channel analysis.** The interfaces between components must be examined for compliance with the security requirements. The examination includes all interfaces with software previously developed (COTS, GOTS, or reuse software). The analysis and evaluation must determine if the identification and authentication, access controls, and discretionary access controls have been implemented correctly and completely.

C4.3.3.2.4.1. The security-critical components of the software, hardware, and firmware and the functions they perform, must be identified. The functional performance of these components must be analyzed and evaluated to determine if the components completely and sufficiently perform the required security functions. **Source code of the security-critical components' interfaces to non-security-critical components must be examined. Fault tree or flaw hypothesis or a similar type of analysis must be used to evaluate any vulnerabilities disclosed by the evaluation.** Any discrepancies must be evaluated as potential security vulnerabilities. This examination must include software applications, software routines, O/S features, firmware, and hardware capabilities critical to maintaining the security (confidentiality, integrity, availability, and accountability) standards necessary for certification and accreditation.

C4.3.3.2.4.2. If a TCB has been integrated into the system, the boundaries must be examined to ensure that they are clearly defined and the integrity of the TCB is maintained in its interaction with other system components. The examination must determine that only external interfaces are used by non-TCB elements to access the TCB. **The examination must ensure that the TCB uses only**

external interfaces to access non-TCB modules or TCB modules in a distributed architecture.

C4.3.3.3. Prerequisite Tasks. Task 2-1.

C4.3.3.4. Input. SSAA, System and Security Architecture, System Design Documentation, and Task 2-1 System Architecture Analysis Summary Report.

C4.3.3.5. Output/Products. The Software, Hardware, and Firmware Analysis Summary Report must be prepared. This report must include the information shown in Table C4.T2.

C4.3.3.6. Suggested References.

C4.3.3.6.1. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C4.3.3.6.2. "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards" (NIST Special Publication 500-165) (reference (v))

C4.3.3.6.3. "Computer Security Considerations in Federal Procurements" (NIST Special Publication 800-4) (reference (o))

C4.3.3.6.4. "Automated Tools for Testing Computer System Vulnerability" (NIST Special Publication 800-6) (reference (w))

C4.3.3.6.5. "Systems Engineering Management Guide" (Defense Systems Management College, January 1990) (reference (n))

C4.3.3.6.6. "A Guide to Understanding Audit in Trusted Systems" (NCSC-TG-001, Version 2) (reference (x))

C4.3.3.6.7. "A Guide to Understanding Discretionary Access Control in Trusted Systems" (NCSC-TG-003) (reference (y))

C4.3.3.6.8. "A Guide to Understanding Design Documentation in Trusted Systems" (NCSC-TG-021, Version 1) (reference (r))

C4.3.3.6.9. "Trusted Network Interpretation Environments Guideline" (NCSC-TG-011, Version 1) (reference (s))

C4.3.3.6.10. "A Guide to Understanding Identification and Authentication in Trusted Systems" (NCSC-TG-017) (reference (z))

C4.3.3.6.11. "A Guide to Understanding Object Reuse in Trusted Systems" (NCSC-TG-018) (reference (aa))

C4.3.3.6.12. "Trusted Database Management System Interpretation" (NCSC-TG-012) (reference (p))

C4.3.3.6.13. "A Guide to Understanding Trusted Recovery in Trusted Systems" (NCSC-TG-022) (reference (t))

C4.3.3.6.14. "Assessing Controlled Access Protection" (NCSC-TG-028) (reference (q))

C4.3.4. Task 2-3, Network Connection Rule Compliance Analysis.

C4.3.4.1. Task Objective. The objective of this task is to evaluate the connections to other systems and/or networks to ensure that network and overall system security policies are enforced.

C4.3.4.2. Task Description. This task evaluates the intended connections to other systems and networks to ensure the system design will enforce specific network security policies and protect the IS from adverse confidentiality, integrity, availability, and accountability impacts. The connection of an IS to a network requires that the particular system will not adversely affect the network's security posture. Connection also requires that the network will not adversely affect the IS's own security posture.

C4.3.4.2.1. Network analysis may include the evaluation of intended interfaces for compliance with the security connection rules not only for the network, but also for the IS. The system CONOPS must be examined to identify all the connections and interfaces intended for the system. It is important to determine if connections exist that were not in the initial concept, but added after the initial fielding or modification of the system. The interfaces to the networks or other systems must be evaluated to determine if the system and network security can be maintained at both ends of the interface. They must also be evaluated to ensure that end-to-end connection constructs are maintained and security connection rules are applied.

C4.3.4.2.2. Level 1. Complete the Minimal Security Activity Checklist.

C4.3.4.2.3. Level 2. Complete the Minimal Security Activity Checklist. Analyze the system interfaces with networks or other systems and evaluate them for compliance with the security connection rules. The system CONOPS must be examined to identify all the connections and interfaces intended for the system. It is also important to determine if additional connections are planned that are not in the initial concept, but are intended to be added sometime after the system's initial fielding. The interfaces to the networks or to other systems must be evaluated to determine that the security of systems and networks at both ends of the interface are maintained. Test plans and procedures should be developed.

C4.3.4.2.4. Level 3. Complete the Minimal Security Activity Checklist. Analyze the system interfaces with networks or other systems and evaluate them for compliance with the security connection rules. The system CONOPS must be examined to identify all the connections and interfaces intended for the system. It is also important to determine if additional connections are planned that are not in the initial concept, but are intended to be added sometime after the system's initial fielding. The interfaces to the networks or to other systems must be evaluated to determine that the security of systems and networks at both ends of the interface are maintained. **The system design must be examined to verify that the interfaces identified comply with the connection rules. Test plans and procedures must be developed to validate compliance with the network connection rules.**

C4.3.4.2.4.1. **The security test plans and procedures must be structured to evaluate the effectiveness of the security features and ensure that there are no methods of circumventing these features. The test plans and procedures for network or system interfaces must demonstrate that the network security policies and procedures are in place and functional.**

C4.3.4.2.5. Level 4. Complete the Minimal Security Activity Checklist. Analyze the system interfaces with networks or other systems and evaluate them for compliance with the security connection rules. The system CONOPS must be examined to identify all the connections and interfaces intended for the system. It is also important to determine if additional connections are planned that are not in the initial concept, but are intended to be added sometime after the system's initial fielding. The interfaces to the networks or to other systems must be evaluated to determine that the security of systems and networks at both ends of the interface are maintained. The system design must be examined to verify that the interfaces identified comply with the connection rules. Test plans and procedures must be developed to validate compliance with the network connection rules.

C4.3.4.2.5.1. The security test plans and procedures must be structured to evaluate the effectiveness of the security features and ensure that there are no methods of circumventing these features. The test plans and procedures for network or system interfaces must demonstrate that the network security policies and procedures are in place and functional.

C4.3.4.3. Prerequisite Tasks. Tasks 2-1 and 2-2.

C4.3.4.4. Input. SSAA, Task 2-1 System Architecture Analysis Summary Report and Task 2-2 Software, Hardware, and Firmware Analysis Summary Report.

C4.3.4.5. Output/Products. A Network Compliance Summary Report must be prepared. This report must include the information shown in Table C4.T2.

C4.3.4.6. Suggested References.

C4.3.4.6.1. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C4.3.4.6.2. "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards" (NIST Special Publication 500-165) (reference (v))

C4.3.4.6.3. "Automated Tools for Testing Computer System Vulnerability" (NIST Special Publication 800-6) (reference (w))

C4.3.4.6.4. "Systems Engineering Management Guide" (Defense Systems Management College, January 1990) (reference (n))

C4.3.4.6.5. "A Guide to Understanding Audit in Trusted Systems" (NCSC-TG-001) (reference (x))

C4.3.4.6.6. "A Guide to Understanding Discretionary Access Control in Trusted Systems" (NCSC-TG-003) (reference (y))

C4.3.4.6.7. "A Guide to Understanding Design Documentation in Trusted Systems" (NCSC-TG-021) (reference r))

C4.3.4.6.8. "Trusted Network Interpretation Environments Guideline" (NCSC-TG-011, Version 1) (reference (s))

C4.3.4.6.9. "A Guide to Understanding Identification and Authentication in Trusted Systems" (NCSC-TG-017, Version 1) (reference (z))

C4.3.4.6.10. "A Guide to Understanding Object Reuse in Trusted Systems" (NCSC-TG-018) (reference (aa))

C4.3.4.6.11. "Trusted Database Management System Interpretation" (NCSC-TG-012) (reference (p))

C4.3.4.6.12. "A Guide to Understanding Trusted Recovery in Trusted Systems" (NCSC-TF-022) (reference (t))

C4.3.4.6.13. "Assessing Controlled Access Protection" (NCSC-TG-028) (reference (q))

C4.3.5. Task 2-4, Integrity Analysis of Integrated Products.

C4.3.5.1. Task Objective. The objective of this task is to evaluate the integration of COTS, GOTS, or Non-Developmental Item (NDI) software, hardware, and firmware to ensure that their integration into the system design complies with the system security architecture and the integrity of each product is maintained.

C4.3.5.2. Task Description. Integrity analysis of products being integrated into the system must identify the security functionality of each product. The certification team should verify the product security functionality to confirm that the needed security functions are present and properly integrated into the system. This task determines whether or not evaluated products are being used for their intended purpose. Product integrity analyses must include an examination of system and subsystem interfaces, product evaluations by the National Institute of Standards and Technology (NIST) or the National Computer Security Center (NCSC), information flows, and applicable use of selected product features.

C4.3.5.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C4.3.5.2.2. Level 2. Complete the Minimal Security Activity Checklist. Determine and document the security functionality of each product. If the product has been obtained from the EPL or undergone a Common Criteria (CC) evaluation, the evaluation results must be examined to ascertain that the product is being used in the manner for which it was evaluated. If the product was obtained from another certified system, the operational scenario and mission must be examined to

ensure that they are consistent with the parent system. System level interfaces must be examined and evaluated to determine that the integrity of the product has been maintained.

C4.3.5.2.3. Level 3. Complete the Minimal Security Activity Checklist. Determine and document the security functionality of each product. If the product has been obtained from the EPL or undergone a CC evaluation, the evaluation results must be examined to ascertain that the product is being used in the manner for which it was evaluated. If the product was obtained from another certified system, the operational scenario and mission must be examined to ensure that they are consistent with the parent system. **Preservation of product integrity analysis must include configuration control of hardware and firmware components, examination of system and subsystem interfaces, examination of product evaluations by NIST or NCSC, information flows, and applicable use of selected product features. The task must verify that the integrity of each product is maintained when interfaced with the system.**

C4.3.5.2.4. Level 4. Complete the Minimal Security Activity Checklist. Determine and document the security functionality of each product. If the product has been obtained from the EPL or undergone CC evaluation, the evaluation results must be examined to ascertain that the product is being used in the manner for which it was evaluated. If the product was obtained from another certified system, the operational scenario and mission must be examined to ensure that they are consistent with the parent system. Preservation of product integrity analysis must include configuration control of hardware and software components, examination of system and subsystem interfaces, examination of product evaluations by NIST or NCSC, information flows, and applicable use of selected product features. **All interfaces and information flows must be examined to determine that only external interfaces are used to access the product.** The task must verify that the integrity of each product is maintained when interfaced with the system.

C4.3.5.3. Prerequisite Tasks. Tasks 2-1 and 2-2.

C4.3.5.4. Input. SSAA, Task 2-1 System Architecture Analysis Summary Report and Task 2-2 Software, Hardware, and Firmware Analysis Summary Report.

C4.3.5.5. Output/Products. Integrated Products Analysis Summary Report must be prepared. This report must include the information shown in Table C4.T2.

C4.3.5.6. Suggested References.

C4.3.5.6.1. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C4.3.5.6.2. "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards" (NIST Special Publication 500-165) (reference (v))

C4.3.5.6.3. "Automated Tools for Testing Computer System Vulnerability" (NIST Special Publication 800-6) (reference (w))

C4.3.5.6.4. "Systems Engineering Management Guide" (Defense Systems Management College, January 1990) (reference (n))

C4.3.5.6.5. "A Guide to Understanding Audit in Trusted Systems" (NCSC-TG-001, Version 2) (reference (x))

C4.3.5.6.6. "A Guide to Understanding Discretionary Access Control in Trusted Systems" (NCSC-TG-003, Version 1) (reference (y))

C4.3.5.6.7. "A Guide to Understanding Design Documentation in Trusted Systems" (NCSC-TG-021, Version 1) (reference (r))

C4.3.5.6.8. "Trusted Network Interpretation Environments Guideline" (NCSC-TG-011, Version 1) (reference (s))

C4.3.5.6.9. "A Guide to Understanding Identification and Authentication in Trusted Systems" (NCSC-TG-017, Version 1) (reference (z))

C4.3.5.6.10. "A Guide to Understanding Object Reuse in Trusted Systems" (NCSC-TG-018, Version 1) (reference (aa))

C4.3.5.6.11. "Trusted Database Management System Interpretation" (NCSC-TG-012) (reference (p))

C4.3.5.6.12. "A Guide to Understanding Trusted Recovery in Trusted Systems" (NCSC-TG-011, Version 1) (reference (t))

C4.3.5.6.13. ""Assessing Controlled Access Protection" (NCSC-TG-028) (reference (q))

C4.3.6. Task 2-5, Life-Cycle Management Analysis.

C4.3.6.1. Task Objective. The objective of this task is to evaluate the ability of configuration management (CM) practices to preserve the integrity of the identified security-relevant software and hardware.

C4.3.6.2. Task Description. This task analyzes the system life-cycle management plans to determine that CM practices are, or will be, in place and are sufficient to preserve the integrity of the security relevant software and hardware. In some cases, the security requirements may dictate special needs for the development environment and the development or integration team (cleared facilities or cleared programmers). If this is the case, the development approach, procedures, and engineering environment are assessed during the system development. This process may require examining the types of documents or procedures shown in Table C4.T3.

Table C4.T3. System Life-Cycle Management Documentation

1.	Life-Cycle Management Plan.
2.	Configuration Identification Procedures.
3.	Configuration Control Procedures.
4.	Configuration Status Accounting Procedures.
5.	Configuration Audit Procedures and Reports.
6.	Software Engineering (development approach and engineering environment) Procedures.
7.	Trusted Distribution Plans.

C4.3.6.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C4.3.6.2.2. Level 2. Complete the Minimal Security Activity Checklist. Evaluate the Life-Cycle Configuration Management Plan and developmental (contractor or Government) CM plan. The CM practices must preserve the integrity of the identified security relevant software and hardware.

C4.3.6.2.3. Level 3. Complete the Minimal Security Activity Checklist. Evaluate the Life-Cycle Configuration Management Plan and developmental (contractor or Government) CM plan. The CM practices must preserve the integrity of the identified security relevant software and hardware. **The task must determine whether CM procedures are in place and are used. A Functional Configuration Audit (FCA) and Physical Configuration Audit (PCA) of security components must be performed. (These audits may be completed in conjunction with or as part of similar system audits.) The FCA and PCA must verify the configuration items against the SSAA, the development CM plan, and the security test configuration.**

C4.3.6.2.4. Level 4. Complete the Minimal Security Activity Checklist. Evaluate the Life-Cycle Configuration Management Plan and developmental (contractor or Government) CM plan. The CM practices must preserve the integrity of the identified security relevant software and hardware. The task must determine whether CM procedures are in place and are used. **CM of system administration documentation, automated tools, and security test cases must be analyzed and evaluated.** An FCA and PCA of security components must be performed. (These audits may be completed in conjunction with or as part of, similar system audits.) The FCA and PCA must verify the configuration items against the SSAA, the development CM plan, and the security test configuration.

C4.3.6.3. Prerequisite Tasks. None.

C4.3.6.4. Input. Life-Cycle Management Plan, Configuration Identification Procedures, Configuration Control Procedures, Configuration Status Accounting Procedures, Configuration Audit Procedures and Reports, Software Engineering Procedures, and Trusted Distribution Plans.

C4.3.6.5 Output/Products. A Life-Cycle Management Analysis Summary Report must be prepared. This report must include the information shown in Table C4.T2.

C4.3.6.6. Suggested References.

C4.3.6.6.1. "Configuration Management Military Standard" (MIL-STD-973) (reference (ab))

C4.3.6.6.2. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C4.3.6.6.3. "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards" (NIST Special Publication 500-165) (reference (v))

C4.3.6.6.4. "Systems Engineering Management Guide" (Defense Systems Management College, January 1990) (reference (n))

C4.3.6.6.5. "A Guide to Understanding Audit in Trusted Systems" (NCSC-TG-001, Version 2) (reference (x))

C4.3.6.6.6. "A Guide to Understanding Configuration Management in Trusted Systems" (NCSC-TG-006, Version 1) (reference (ac))

C4.3.6.6.7. "A Guide to Understanding Design Documentation in Trusted Systems" (NCSC-TG-021, Version 1) (reference (r))

C4.3.6.6.8. "A Guide to Understanding Trusted Distribution in Trusted Systems" (NCSC-TG-008, Version 1) (reference (ad))

C4.3.6.6.9. "Trusted Network Interpretation Environments Guideline" (NCSC-TG-011, Version 1) (reference (s))

C4.3.6.6.10. "Rating Maintenance Phase Program Documentation" (NCSC-TG-013) (reference (ae))

C4.3.6.6.11. "A Guide to Understanding Trusted Facility Management" (NCSC-TG-015, Version 1) (reference (af))

C4.3.6.6.12. "A Guide to Understanding Object Reuse in Trusted Systems" (NCSC-TG-018, Version 1) (reference (aa))

C4.3.6.6.13. "Trusted Database Management System Interpretation" (NCSC-TG-012) (reference (p))

C4.3.7. Task 2-6, Security Requirements Validation Procedures.

C4.3.7.1. Task Objective. The objective of this task is to prepare the written procedures used in Phase 3 to validate compliance with the technical security requirements.

C4.3.7.2. Task Description. In this task, the certification team writes the procedures to be used in Phase 3 to validate compliance with all the defined technical security requirements. The security requirements document should identify the type of review required to validate each requirement: test, observation, review, or interview. Many organizations use an RTM to identify the applicable security requirements and the appropriate method to validate those requirements. At certification Level 1, the test procedures may be a detailed checklist. At certification Levels 2 through 4, a test, observation, review, or interview should verify compliance with each requirement. If test procedures are prepared, they should be added to the SSAA.

C4.3.7.2.1. Level 1. Verify the questions in the Minimum Security Checklist are appropriate to evaluate the system. Add additional questions to the checklist to completely assess the system and components being accredited.

C4.3.7.2.2. Level 2. Identify the most appropriate way to validate each security requirement identified in the RTM: test, observation, review, or interview. If test plans are required, the certification team should prepare a Test Plans and Procedures document. Test procedures should be written for each requirement to be tested. The test procedures should follow the format recommended in Table C4.T4.

Table C4.T4. Test Procedure Format

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

C4.3.7.2.3. Level 3. Identify the most appropriate way to validate each security requirement identified in the RTM: test, observation, review, or interview. If test plans are required, the certification team should prepare a Test Plans and Procedures document. Test procedures should be written for each requirement to be tested. The test procedures should follow the format recommended in Table C4.T4.

C4.3.7.2.4. Level 4. Identify the most appropriate way to validate each security requirement identified in the RTM: test, observation, review, or interview. If test plans are required, the certification team should prepare a Test Plans and Procedures document. Test procedures should be written for each requirement to be tested. The test procedures should follow the format recommended in Table C4.T4.

C4.3.7.3. Prerequisite Tasks. Task 2-1 through Task 2-5.

C4.3.7.4. Input. Minimum Security Checklist, Task Summary Reports from prerequisite tasks, System Design Documentation.

C4.3.7.5. Output/Products. Customized Minimum Security Checklist, Test plans and procedures.

C4.3.7.6. Suggested References. None.

C4.3.8. Task 2-7, Vulnerability Assessment.

C4.3.8.1. Task Objective. The objective of this task is to evaluate security vulnerabilities (confidentiality, integrity, availability, and accountability), evaluate residual risk, and recommend appropriate countermeasures.

C4.3.8.2. Task Description. This certification task evaluates security vulnerabilities with regard to confidentiality, integrity, availability, and accountability and recommends applicable countermeasures. The Certifier will use this information for preparing the risk assessment. The DAA should determine the acceptable level of risk to protect the system commensurate with its value to the Department of Defense.[10] In Phase 2, the vulnerability assessment concentrates on the sufficiency to the specified technical security requirements to protect and secure the information resources.

C4.3.8.2.1. During vulnerability assessment, each of the vulnerabilities and discrepancies identified 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 by any related threat. The analysis should use techniques such as static penetration, flaw hypothesis, and threat-vulnerability pairing. The design level risk assessment will 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 risks must be identified and evaluated. The evaluation should indicate the operational impacts associated with these risks. Appropriate countermeasures must be determined for each of the high-risk vulnerabilities.

C4.3.8.2.2. Level 1. Complete the Minimal Security Activity Checklist.

---

10 An acceptable level of residual risk is based on the relationship of the threat to the system and the information processed; to the IS's mission, environment, and architecture; and its security confidentiality, integrity, availability, and accountability (authenticity and nonrepudiation) objectives.

C4.3.8.2.3. Level 2. Complete the Minimal Security Activity Checklist. Examine the task summary reports and evaluate the vulnerabilities discovered during those evaluations. The criticality of the vulnerabilities must be assessed and the vulnerabilities rank ordered with respect to ease of exploitation and potential rewards to the exploiter. All results must be documented and consolidated into a draft certification package.

C4.3.8.2.4. Level 3. Complete the Minimal Security Activity Checklist. Examine the task summary reports and evaluate the vulnerabilities discovered during those evaluations. The criticality of the vulnerabilities must be assessed and the vulnerabilities rank ordered with respect to ease of exploitation and potential rewards to the exploiter. **Countermeasures must be proposed to offset the risk of vulnerabilities.** All results must be documented and consolidated into a draft certification package.

C4.3.8.2.5. Level 4. Complete the Minimal Security Activity Checklist. Examine the task summary reports and evaluate the vulnerabilities discovered during those evaluations. The criticality of the vulnerabilities must be assessed and the vulnerabilities rank ordered with respect to ease of exploitation and potential rewards to the exploiter. Countermeasures must be proposed to offset the risk of each vulnerability. **A cost to implement each proposed countermeasure versus risk tradeoff analysis must be performed.** All results must be documented and consolidated into a draft certification package.

C4.3.8.3. Prerequisite Tasks. Task 2-1 through Task 2-6.

C4.3.8.4. Input. Task Summary Reports from prerequisite tasks, System Design Documentation, Preliminary Design Review (PDR) and Critical Design Review (CDR) Results, Source Code, IV&V Reports.

C4.3.8.5. Output/Products. A Vulnerability Assessment Report must be prepared.

C4.3.8.6. Suggested References.

C4.3.8.6.1. "Guidelines for Automatic Data Processing Physical and Risk Management" (FIPS Publication 31) (reference (ag))

C4.3.8.6.2. "Guideline for Automatic Data Processing Risk Analysis" (FIPS Publication 65) (reference (ah))

C4.3.8.6.3. "Configuration Management Military Standard" (MIL-STD-973) (reference (ab))

C4.3.8.6.4. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C4.3.8.6.5. "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project management Standards" (NIST Special Publication 500-165) (reference (v))

C4.3.8.6.6. "Automated Tools for Testing Computer System Vulnerability" (NIST Special Publication 800-6) (reference (w))

C4.3.8.6.7. "Systems Engineering Management Guide" (Defense Systems Management College, January 1990) (reference (n))

C4.3.8.6.8. "A Guide to Understanding Audit in Trusted Systems" (NCSC-TG-001, Version 2) (reference (x))

C4.3.8.6.9. "A Guide to Understanding Discretionary Access Control in Trusted Systems" (NCSC-TG-003, Version 1) (reference (y))

C4.3.8.6.10. "A Guide to Understanding Configuration Management in Trusted Systems" (NCSC-TG-006, Version 1) (reference (ac))

C4.3.8.6.11. "A Guide to Understanding Design Documentation in Trusted Systems" (NCSC-TG-021, Version 1) (reference (r))

C4.3.8.6.12. "A Guide to Understanding Trusted Distribution in Trusted Systems" (NCSC-TG-008, Version 1) (reference (ad))

C4.3.8.6.13. "Rating Maintenance Phase Program Documentation" (NCSC-TG-013) (reference (ae))

C4.3.8.6.14. "A Guide to Understanding Trusted Facility Management" (NCSC-TG-015, Version 1) (reference (af))

C4.3.8.6.15. "A Guide to Understanding Identification and Authentication in Trusted Systems" (NCSC-TG-017, Version 1) (reference (z))

C4.3.8.6.16. "A Guide to Understanding Object Reuse in Trusted Systems" (NCSC-TG-018, Version 1) (reference (aa))

C4.3.8.6.17. "Trusted Database Management System Interpretation" (NCSC-TG-012) (reference (p))

C4.3.8.6.18. "A Guide to Understanding Trusted Recovery in Trusted Systems" (NCSC-TF-022) (reference (t))

C4.3.8.6.19. "Assessing Controlled Access Protection" (NCSC-TG-028) (reference (q))

C4.4. PHASE 2 ROLES AND RESPONSIBILITIES

C4.4.1. Security Team Responsibilities.

C4.4.1.1. DAA Responsibilities. The DAA must continuously review the system for compliance with the SSAA. In the Verification Phase, the DAA oversees the evaluation of the system. The DAA also reviews the SSAA to ensure it accurately describes the system, the threat, environment, security requirements, system vulnerabilities, and all conditions under which the system will be operated.

C4.4.1.2. Certifier and Certification Team. The Certifier conducts a technical and nontechnical evaluation of the system. In Phase 2, the Certifier or certification team is responsible for the activities shown in Table C4.T5.

Table C4.T5. Certifier and Certification Team Responsibilities

1.	Conduct the Phase 2 certification analysis tasks.
2.	Identify and assess system vulnerabilities.
3.	Report certification results to the DAA, program manager, and user representative.
4.	Provide advice to the DAA, program manager, and user representative regarding the readiness of the system to move into the Validation Phase.
5.	Maintain C&A schedules, plan of action, and milestones based on performance of the technical effort.
6.	Integrate changes into the SSAA.

C4.4.1.3. ISSO Responsibilities. During Phase 2, the ISSO is responsible for the tasks shown in Table C4.T6.

Table C4.T6. ISSO Responsibilities

1.	Review the mission statement to determine if it accurately describes the system.
2.	Review the environment description to determine if it accurately describes the system.

C4.4.2. User Representative Responsibilities. During Phase 2, the user representative is responsible for the tasks shown in Table C4.T7.

Table C4.T7. User Representative Responsibilities

1.	Support certification actions.
2.	Prepare Security Rules of Behavior and Standard Operating Procedures.
3.	Provide changes to the mission statement, functional environment, and organizational structure to the certification team.
4.	Verify the feasibility of security solutions and the ability to comply in the operational environment.

C4.4.3. Acquisition or Maintenance Organization Responsibilities.

C4.4.3.1. Program Manager Responsibilities. The program manager is responsible for development of the system. During Phase 2, the program manager is responsible for the tasks show in Table C4.T8.

Table C4.T8. Program Manager Responsibilities

1.	Develop system or system modifications.
2.	Support the certification efforts by providing updates on the mission statement, environmental description, and architectural changes.
3.	Review the certification results.
4.	Make system modifications as necessary to reduce or eliminate system vulnerabilities.

C4.4.3.2. Program Management Support Staff Responsibilities. The program management support staff perform the tasks shown in Table C4.T9 during Phase 2.

Table C4.T9. Program Management Support Staff Responsibilities

1.	Determinate the level of effort.
2.	Support cost and schedule determinations.
3.	Monitor progress.
4.	Maintain system documentation.

C4.4.3.3. Developer, Integrator, or Maintainer Responsibilities. During Phase 2 the developer, integrator, or maintainer is responsible for the tasks shown in Table C4.T10.

Table C4.T10. Developer, Integrator or Maintainer Responsibilities

1.	Provide hardware and software architecture to the acquisition organization.
2.	Provide technical equipment environment requirements to the acquisition organization.
3.	Develop or integrate technical security solutions and security requirements.

C4.4.3.4. Configuration Management Responsibilities. During Phase 2, the configuration management staff supports the program manager in the development and maintenance of system documentation.

C4.4.3.5. System Administration. There are no system administration responsibilities in Phase 2.

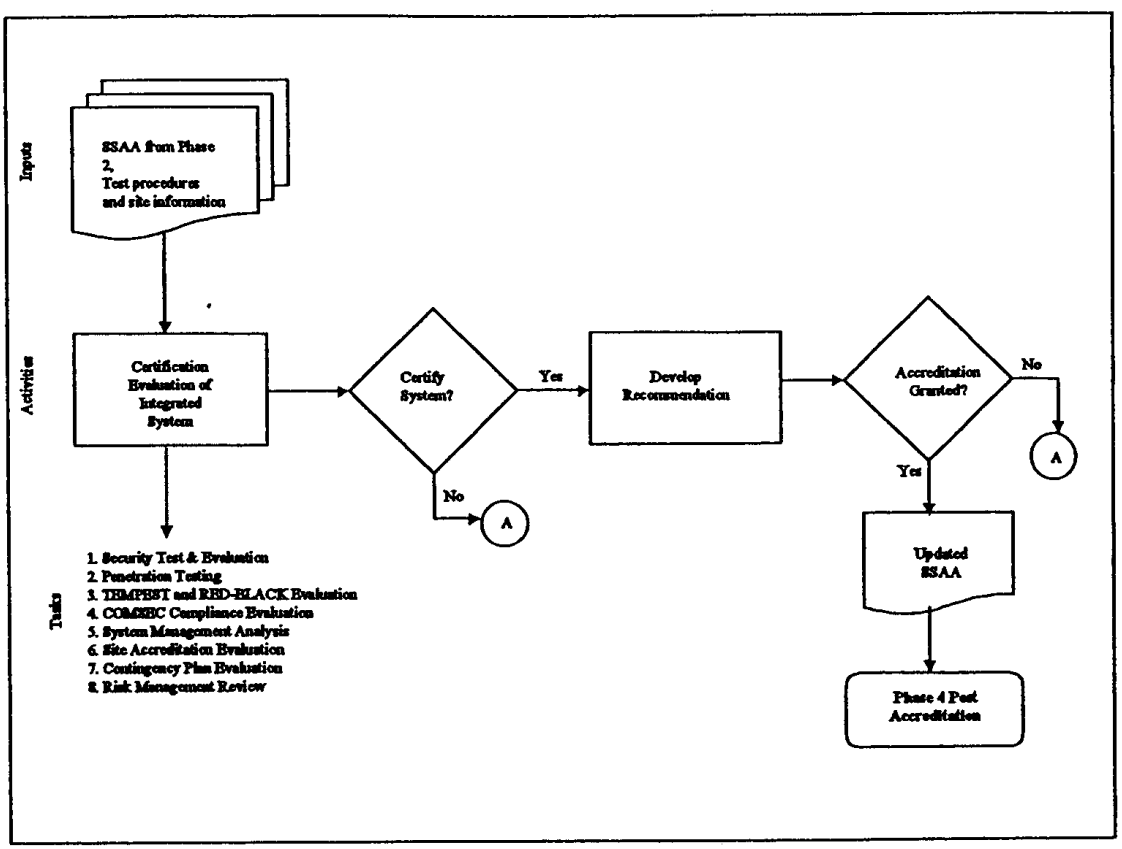
C5. CHAPTER 5

PHASE 3, VALIDATION

C5.1. PHASE 3 OVERVIEW

C5.1.1. Phase 3 activities, Figure C5.F1., validate that the preceding work has produced an IS that operates in a specified computing environment with an acceptable level of residual risk. This phase consists of activities that occur after the system is integrated and culminates in the accreditation of the IS. Phase 3 includes a review of the SSAA, an evaluation of the integrated IS, certification, and accreditation.

Figure C5.F1. Validation Phase



C5.1.2. Phase 3 certification tasks include certification of software, firmware, hardware, and inspections of operational sites to ensure their compliance with physical security, procedural security, TEMPEST and COMSEC requirements, personnel

security, and security education, training, and awareness requirements. Phase 3 includes tasks to certify the compatibility of the computing environment with the description provided in the SSAA. DITSCAP flexibility permits the certification actions to be scaled to the type of IS being evaluated and tailored to the program strategy used in the development or modification of the system.

C5.1.3. Each IS must be covered by an SSAA. In some cases a single SSAA may include several systems. For type accreditation's, an SSAA may be prepared for the system software and hardware considered under the type accreditation. This SSAA should be shipped to each prospective installation site with the software and hardware. The site manager will receive confirmation and documentation of the C&A results and the equipment included in the SSAA. After installation of the IS, the information from the type SSAA should be included in the target system's (network or site) SSAA. The system configuration and security environment must still be certified during Phase 3.

C5.2. PHASE 3 ACTIVITIES

C5.2.1. SSAA Refinement. Phase 3 begins with a review of the SSAA to ensure that its requirements and agreements still apply. That review continues throughout Phase 3. At each stage of the validation process, details are added to the documents reflecting the current state of the system. Required changes must be submitted to the DAA, Certifier, program manager, and user representative so the revised agreement may be approved and implemented.

C5.2.2. Certification Evaluation of the Integrated System. This activity certifies that the fully integrated and operational system will comply with the requirements stated in the SSAA and the system will be operated with an acceptable level of residual risk. During this activity, certification tasks are performed to ensure that the IS is functionally ready for operations. The certification tasks and the extent of the tasks will depend on the level of certification analysis in the SSAA. The certification tasks are listed in Table C5.T1.

Table C5.T1. Phase 3, Validation Tasks

1.	Security Test and Evaluation
2.	Penetration Testing
3.	TEMPEST and RED-BLACK Evaluation
4.	COMSEC Compliance Evaluation
5.	System Management Analysis
6.	Site Accreditation Survey
7.	Contingency Plan Evaluation
8.	Risk Management Review

C5.2.2.1. As each task is completed, the results are evaluated and documented. The Certifier must evaluate the tasks for completeness and determine if the activity is consistent with the approach stated in the SSAA. The results of the completed task analysis are then documented and added to the SSAA. If problems occur while evaluating the integrated system, the Certifier must notify the program manager. If the problem can be fixed, the Certifier can repeat the task analysis activity. The problem and the solution must be included as part of the findings.

C5.2.3. Recommendation to DAA. This activity begins after completion of all certification tasks and ends with a system accreditation recommendation. The purposes of this activity are to consolidate the findings developed during certification of the integrated system and submit the Certifier's report to the DAA.

C5.2.3.1. If the Certifier concludes that the integrated IS satisfies the SSAA technical requirements, the Certifier issues a system certification. The systems certification certifies that the IS has complied with the documented security requirements. Supplemental recommendations might also be made to improve the system's security posture. Such recommendations should provide input to future system enhancements and configuration management decisions.

C5.2.3.2. In some cases, the Certifier may uncover security deficiencies, but continue to believe that the short-term system operation is within the bounds of acceptable risk. The Certifier may recommend an Interim Approval To Operate (IATO) with the understanding that deficiencies will be corrected in a time period specified by the DAA. These deficiencies must be reflected in the SSAA and an agreement obtained on the conditions under which the system may be operated and the date by when the deficiencies will be remedied.

C5.2.3.3. If the Certifier determines that the system does not satisfy the

security requirements and that short-term risks place the system operation or information in jeopardy, the Certifier must recommend that the IS not be accredited.

C5.2.4. DAA Accreditation Decision. After receipt of the Certifier's recommendation, the DAA reviews the SSAA and makes an accreditation determination. This determination is added to the SSAA. The final SSAA accreditation package includes the Certifier's recommendation, the DAA authorization to operate, and supporting documentation. The SSAA must contain all the information necessary to support the Certifier's recommendation including security findings, deficiencies, risks to operate, and actions to resolve any deficiencies.

C5.2.4.1. If the decision is to accredit, the decision must include the security parameters under which the IS is authorized to operate. If the system does not meet the requirements stated in the SSAA, but mission criticality mandates that the system become operational, an IATO may be issued. The DAA, Certifier, program manager, and user representative must agree to the proposed solutions, schedule, security actions, milestones, and maximum length of time for the IATO validity.

C5.2.4.2. When the system accreditation has been issued, the responsibility for the SSAA will move to the ISSO. When a decision is made to accredit the system, the DITSCAP begins Phase 4. If the DAA withholds accreditation, the decision must state the specific reasons for denial and, if possible, provide suggested solutions. The DITSCAP then reverts to Phase 1 to resolve the issues.

C5.2.4.3. In some situations a common set of software, hardware, and firmware is installed at multiple locations. Since it is difficult to accredit the common systems at all possible locations, the DAA may issue a type accreditation for a typical operating environment. The type accreditation is the official authorization to employ identical copies of a system in a specified environment. The SSAA must be modified to include a statement of residual risk and clearly define the intended operating environment. The SSAA must identify specific uses of the system, operational constraints and procedures under which the system may operate. In that case, the DAA would include a statement with the accreditation, such as, "This system is supplied with a type accreditation. With the type accreditation, the operators assume the responsibility to monitor the environment for compliance with the environment as described in the accreditation documentation." The program manager, user representative, and ISSO should ensure that the proper security operating procedures, configuration guidance, and training is delivered with the system.

C5.3. PHASE 3 CERTIFICATION TASKS

C5.3.1. Phase 3 Task Overview. During Phase 3, eight certification tasks are performed on the integrated operational system to ensure that the IS is functionally ready for operational deployment. The certification tasks and the extent of the tasks will depend on the certification level agreed on in the SSAA. After each task is completed, a Task Analysis Summary Report must be prepared. This report must include the information shown in Table C5.T2. For each task and level, complete the Minimum Security Checklist, Appendix 2.

Table C5.T2. Task Analysis Report Topics

1.	Record of findings.
2.	Evaluation of vulnerabilities discovered during evaluations.
3.	Summary of the analysis level of effort.
4.	Summary of tools used and results obtained.
5.	Recommendations.

C5.3.2. Task 3-1, Security Test and Evaluation (ST&E).

C5.3.2.1. Task Objective. The objective of this task is to evaluate the technical implementation of the security design and to ascertain that security software, hardware, and firmware features affecting confidentiality, integrity, availability, and accountability have been implemented as documented in the SSAA and that the features perform properly.

C5.3.2.2. Task Description. ST&E validates the correct implementation of identification and authentication, audit capabilities, access controls, object reuse, trusted recovery, and network connection rule compliance. Individual tests evaluate system conformance with the requirements, mission environment, and architecture. Test plans and procedures should address all the security requirements and provide sufficient evidence of the amount of residual risk. These results must validate the proper integration and operation of all security features.

C5.3.2.2.1. Hands-on testing should focus on TCB interfaces, system initialization, shutoff, and aborts to ensure that the system remains in a secure state. Because it is not feasible to include every possible input when testing a system, the tester should select those inputs that exercise every security module or every system security function and place stress on the system. Errors should be introduced to test if the system fails to perform its function when given invalid commands. If network

connections are being used, the team should verify that the connection rules are enforced.

C5.3.2.2.2. When a system is developed for deployment to multiple locations a type accreditation may be desirable. In this situation, a CT&E should occur at a central integration and test facility or at one of the intended operating sites, if such a facility if not available. Software and hardware security tests of common system components at multiple sites are not recommended. At the conclusion of the type accreditation CT&E, the test results, Certifier's recommendation, and the type accreditation are documented in the SSAA. This SSAA is then sent with the software and hardware suite to each site where the IS will be installed. The site will not need to repeat the baseline test conducted by the type accreditation effort. However, the system installation and security configuration should be tested at each operational site in the site ST&E.

C5.3.2.2.3. Level 1. Complete the Minimal Security Activity Checklist.

C5.3.2.2.4. Level 2. Complete the Minimal Security Activity Checklist. Determine if high-level technical (hardware, software, and firmware) security requirements identified in Phase 1 have a corresponding test procedure. The tests should be developed to test the correct implementation of the security policy.

C5.3.2.2.4.1. The security functional testing must evaluate the system to determine that the implemented system meets the security capabilities defined by the SSAA and that the installation parameters and installation procedures are implemented correctly. Tests must validate compliance with the network connection rules.

C5.3.2.2.4.2. The availability and reliability evaluation must check for consistency with the approach stated in the SSAA. This evaluation must determine if the system meets established availability and reliability requirements and ensures that the tested system is a correct functional representation of the operational system(s).

C5.3.2.2.5. Level 3. Complete the Minimal Security Activity Checklist. Determine if high-level technical (hardware, software, and firmware) security requirements identified in Phase 1 have a corresponding test procedure. The tests should be developed to test the correct implementation of the security policy.

C5.3.2.2.5.1. The security functional testing must evaluate the system to determine that the implemented system meets the security capabilities

defined by the SSAA and that the installation parameters and installation procedures are implemented correctly. Tests must validate compliance with the network connection rules. **Security functions must be tested to verify the integration and operation of all security features. The testing must validate the correct implementation of identification and authentication, audit analysis, access controls, object reuse, trusted recovery, discretionary access controls, and network connection rule compliance.**

C5.3.2.2.5.2. **If available, the TFM and SFUG must be validated for correctness. Key procedures in the TFM and SFUG must be evaluated for completeness**.

C5.3.2.2.5.3. The availability and reliability evaluation must check for consistency with the approach stated in the SSAA. This evaluation must determine if the system meets established availability and reliability requirements and ensures that the tested system is a correct functional representation of the operational system(s).

C5.3.2.2.6. Level 4. Complete the Minimal Security Activity Checklist. Determine if **all technical** (hardware, software, and firmware) security requirements identified in Phase 1 have a corresponding test procedure. The tests should be developed to test the correct implementation of the security policy.

C5.3.2.2.6.1. The security functional testing must evaluate the system to determine that the implemented system meets the security capabilities defined by the SSAA and that the installation parameters and installation procedures are implemented correctly. Tests must validate compliance with the network connection rules. Security functions must be tested to verify the integration and operation of all security features. The testing must validate the correct implementation of identification and authentication, audit analysis, access controls, object reuse, trusted recovery, discretionary access controls, and network connection rule compliance.

C5.3.2.2.6.2. **The TFM and SFUG must be validated for correctness. All the procedures in the TFM and SFUG must be evaluated for completeness.**

C5.3.2.2.6.3. The availability and reliability evaluation must check for consistency with the approach stated in the SSAA. This evaluation must determine if the system meets established availability and reliability requirements and

ensures that the tested system is a correct functional representation of the operational system(s).

C5.3.2.3. Prerequisite Tasks. Task 2-1 and Task 2-7.

C5.3.2.4. Input. Test plan and procedures.

C5.3.2.5. Output/Products. An ST&E Analysis Summary Report must be prepared. This report must include the information shown in Table C5.T2.

C5.3.2.6. Suggested References.

C5.3.2.6.1. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C5.3.2.6.2. "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards" (NIST Special Publication 500-165) (reference (v))

C5.3.2.6.3. "Automated Tools for Testing Computer System Vulnerability" (NIST Special Publication 800-6) (reference (w))

C5.3.2.6.4. "A Guide to Understanding Audit in Trusted Systems" (NCSC-TG-001, Version 2) (reference (x))

C5.3.2.6.5. "A Guide to Understanding Discretionary Access Control in Trusted Systems" (NCSC-TG-003, Version 1) (reference (y))

C5.3.2.6.6. "A Guide to Understanding Identification and Authentication in Trusted Systems" (NCSC-TG-021) (reference (r))

C5.3.2.6.7. "A Guide to Understanding Object Reuse in Trusted Systems" (NCSC-TG-018, Version 1) (reference (aa))

C5.3.2.6.8. "Assessing Controlled Access Protection (NCSC-TG-028) (reference (q)).

C5.3.3. Task 3-2, Penetration Testing.

C5.3.3.1. Task Objective. The objective of this task is to assess the system's ability to withstand intentional attempts to circumvent security features through exploitation of the technical security vulnerabilities.

C5.3.3.2. Task Description. Penetration testing is strongly recommended for systems of any complexity or criticality. Penetration testing assesses the system's ability to withstand intentional attempts to circumvent system security features by exploiting technical security vulnerabilities. Penetration testing may include insider and outsider penetration attempts based on common vulnerabilities for the technology being used.

C5.3.3.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C5.3.3.2.2. Level 2. Complete the Minimal Security Activity Checklist.

C5.3.3.2.3. Level 3. **Analyze the penetration testing to evaluate the procedures to determine compliance with the approach stated in the SSAA. The testing must include insider and outsider penetration attempts based on known vulnerabilities. The implemented systems must be tested for flaws, with the results described to an appropriate level for the exploitation.**

C5.3.3.2.4. Level 4. Analyze the penetration testing to evaluate the procedures to determine compliance with the approach stated in the SSAA. The testing must include insider and outsider penetration attempts based on known vulnerabilities. The implemented systems must be tested for flaws, with the results described to an appropriate level for the exploitation.

C5.3.3.3. Prerequisite Tasks. Task 2-1 through Task 2-7.

C5.3.3.4. Input. Vulnerability Assessment Report, IV&V Reports, and Task Summary Reports from all prerequisite tasks.

C5.3.3.5. Outputs/Products. A Penetration Testing Analysis Summary Report must be prepared. This report must include the information shown in Table C5.T2.

C5.3.3.6. Suggested References.

C5.3.3.6.1. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C5.3.3.6.2. "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards" (NIST Special Publication 500-165) (reference (v))

C5.3.3.6.3. "Automated Tools for Testing Computer System Vulnerability" (NIST Special Publication 800-6) (reference (w))

C5.3.3.6.4. "A Guide to Understanding Discretionary Access Control in Trusted Systems" (NCSC-TG-003, Version 1) (reference (y))

C5.3.3.6.5. "A Guide to Understanding Configuration Management in Trusted Systems" (NCSC-TG-006, Version 1) (reference (ac)).

C5.3.3.6.6. "A Guide to Understanding Design Documentation in Trusted Systems" (NCSC-TG-021, Version 1) (reference (r))

C5.3.3.6.7. "A Guide to Understanding Trusted Distribution in Trusted Systems" (NCSC-TG-008, Version 1) (reference (ad))

C5.3.3.6.8. "Trusted Network Interpretation Environments Guideline" (NCSC-TG-011, Version 1) (reference (s))

C5.3.3.6.9. "Rating Maintenance Phase Program Documentation" (NCSC-TG-013) (reference (ae))

C5.3.3.6.10. "A Guide to Understanding Trusted Facility Management" (NCSC-TG-015, Version 1) (reference (af))

C5.3.3.6.11. "A Guide to Understanding Identification and Authentication in Trusted Systems" (NCSC-TG-017, Version 1) (reference (z))

C5.3.3.6.12. "A Guide to Understanding Object Reuse in Trusted Systems" (NCSC-TG-018, Version 1) (reference (aa))

C5.3.3.6.13. "Trusted Database Management System Interpretation" (NCSC-TG-012) (reference (p))

C5.3.3.6.14. "A Guide to Understanding Trusted Recovery in Trusted Systems" (NCSC-TG-022) (reference (t))

C5.3.3.6.15. "Assessing Controlled Access Protection" (NCSC-TG-028) (reference (q))

C5.3.4. Task 3-3, TEMPEST and RED-BLACK Verification.

C5.3.4.1. Task Objective. The objective of this task is to validate that the equipment and site meet the TEMPEST and RED-BLACK requirements. (Conduct only if TEMPEST applies.)

C5.3.4.2. Task Description. TEMPEST and RED-BLACK verification may be required to validate that the equipment and site meet the security requirements. In these situations, the site should be inspected to determine if the environment is adequate and that adequate practices are being followed.

C5.3.4.2.1. Level 1. Not required.

C5.3.4.2.2. Level 2. Analyze the TEMPEST compliance with the approach stated in the SSAA. Evaluate the site to determine if adequate TEMPEST practices are followed to reduce potential TEMPEST transmissions beyond the Physical Control Space (PCS). At a minimum, determine that adequate separation exists between RED and BLACK cables, inspect RED power lines for adequate filtering, inspect RED safety grounds and adherence to minimal grounding criteria, examine potential fortuitous conductors for presence of proper dielectric separators at each PCS or secure area, and for the presence of telephone system isolators.

C5.3.4.2.3. Level 3. Analyze the TEMPEST compliance with the approach states in the SSAA. Evaluate the site to determine if adequate TEMPEST practices are followed to reduce potential TEMPEST transmissions beyond the PCS. At a minimum, determine that adequate separation exists between RED and BLACK cables, inspect RED power lines for adequate filtering, inspect RED safety grounds and adherence to minimal grounding criteria, examine potential fortuitous conductors for presence of proper dielectric separators at each PCS or secure area, and for the presence of telephone system isolators. **Determine the TEMPEST zones for the facility. Inspect the facility and the equipment to determine that the equipment is placed in the proper zones or that TEMPEST equipment is used if the facility is not zoned.**

C5.3.4.2.4. Level 4. Analyze the TEMPEST compliance with the approach stated in the SSAA. Evaluate the site to determine if adequate TEMPEST practices are followed to reduce potential TEMPEST transmissions beyond the PCS. At a minimum, determine that adequate separation exists between RED and BLACK cables, inspect RED power lines for adequate filtering, inspect RED safety grounds and adherence to minimal grounding criteria, examine potential fortuitous conductors for presence of proper dielectric separators at each PCS or secure area, and for the

presence of telephone system isolators. **By walkaway and conduction tests, profile the electromagnetic radiation TEMPEST zone (ERTZ) of all RED systems, cables, and components. Ensure that the ERTZ is within the PCS from a three-dimensional perspective.**

C5.3.4.3. Prerequisite Tasks. None.

C5.3.4.4. Input. Operational equipment's electric specifications, drawings, and detailed theory of operation, facility physical controlled space drawings and equipment location.

C5.3.4.5. Output/Products. A TEMPEST/RED-BLACK Analysis Summary Report must be prepared. This report must include the information shown in Table C5.T2.

C5.3.4.6. Suggested References.

C5.3.4.6.1. "Compromising Emanations Laboratory Test Requirements, Electromagnetics" (NSTISSAM TEMPEST/1-92) (reference (ai))

C5.3.4.6.2. "Compromising Emanations Field Test Requirements, Electromagnetics" (NSTISSAM TEMPEST/1-93) (reference (aj))

C5.3.4.6.3. "Procedures for TEMPEST Zoning" (NSTISSAM TEMPEST/2-92) (reference (ak))

C5.3.4.6.4. "Guidelines for Facility Design and Red-Black Installation" (NACSEM 5203) (reference (al))

C5.3.5. Task 3-4, COMSEC Compliance Verification.

C5.3.5.1. Task Objective. The objective of this task is to validate that appropriate COMSEC approval has been granted. (Conduct only is COMSEC applies.)

C5.3.5.2. Task Description. This task validates that National Security Agency (NSA) approved COMSEC is in use and that COMSEC key management procedures are used. COMSEC analysis evaluates how well the SSAA-defined COMSEC requirements are integrated into the system architecture and site management procedures.

C5.3.5.2.1. Level 1. Not required.

C5.3.5.2.2. Level 2. Analyze the COMSEC key management procedures for compliance with the approach stated in the SSAA and for completeness and compliance with the COMSEC operational and security requirements.

C5.3.5.2.3. Level 3. Analyze the COMSEC key management procedures for compliance with the approach stated in the SSAA and for completeness and compliance with the COMSEC operational and security requirements. **Analyze the COMSEC modules for compliance with the approach stated in the SSAA and for consistency with the system architecture.**

C5.3.5.2.4. Level 4. Analyze the COMSEC key management procedures for compliance with the approach stated in the SSAA and for completeness and compliance with the COMSEC operational and security requirements. Analyze the COMSEC modules for compliance with the approach stated in the SSAA. **The COMSEC modules must be evaluated for consistency with the system architecture and that cryptographic principles are appropriate for particular applications.**

C5.3.5.3. Prerequisite Tasks. None.

C5.3.5.4. Input. Key management plan and procedures, Tailored Functional System Requirements Specifications, embedded COMSEC modules design documentation.

C5.3.5.5. Output/Products. A COMSEC Analysis Summary Report must be prepared. This report must include the information shown in Table C5.T2.

C5.3.5.6. Suggested References.

C5.3.5.6.1. "Communications Security" (COMSEC) (DoD Directive C-5200.5) (reference (am))

C5.3.5.6.2. "Defense Special Security Communications Systems: Security Criteria and Telecommunications Guidance" (DoD C-5030.58-M) (reference (an))

C5.3.5.6.3. "Communications Security (COMSEC) Monitoring" (NTISSD 600) (reference (ao))

C5.3.5.6.4. "INFOSEC Software Engineering Standards and Practices Manual" (NSA DS-80) (reference (ap))

C5.3.6. Task 3-5, System Management Analysis.

C5.3.6.1. Task Objective. The objective of this task is to ensure that system security management procedures are in place, operational, and effective. This task verifies that configuration management policies and programs consider security implications in all modifications to the accredited system baseline and operational concept.

C5.3.6.2. Task Description. The system management infrastructure must be examined to determine whether it adequately supports the maintenance of the environment, mission, and architecture described in the SSAA. Infrastructure components include security policies, system and security management organizations, system operating procedures, security training and awareness, Rules of Behavior, incident response plan and procedures, virus detection, and configuration management organization and processes. These components provide insight into security operations at the site.

C5.3.6.2.1. An effective configuration management program is mandatory if an established security posture is to be maintained. The system management analysis task evaluates the configuration management practices to determine their ability to preserve the integrity of the security relevant software and hardware. A system baseline identifies all hardware, software, and firmware components and external interfaces, supports future security evaluations, and establishes a know reference point from which to make future accreditation decisions. Configuration management practices must include periodic reverification of the system configuration to ensure unauthorized changes have not occurred.

C5.3.6.2.2. Level 1. Complete the Minimal Security Activity Checklist.

C5.3.6.2.3. Level 2. Complete the Minimal Security Activity Checklist. Analyze the security management procedures' compliance with the approach stated in the SSAA. This analysis must include an examination of the roles and responsibilities assigned to the ISSO to ensure that the responsibilities are consistent with the procedures identified in the SSAA. The system and security management organization must be examined to determine the ability of the ISSO to report security incidents and implement security changes. The procedures must include the management hierarchy with respect to the ability of the ISSO to report

security incidents and implement changes, management procedures, self-assessment techniques, and security intrusion detection.

C5.3.6.2.4. Level 3. Complete the Minimal Security Activity Checklist. Analyze the security management procedures' compliance with the approach stated in the SSAA. This analysis must include an examination of the roles and responsibilities assigned to the ISSO to ensure that the responsibilities are consistent with the procedures identified in the SSAA. The system and security management organization must be examined to determine the ability of the ISSO to report security incidents and implement security changes.

C5.3.6.2.4.1. **An effective configuration management program is mandatory if an established secure posture is to be maintained. Evaluate the configuration management practices to determine their ability to preserve the integrity of the security relevant software and hardware. A system baseline that identifies all information hardware, software, and firmware components and external interfaces provides for future security evaluations and establishes a known reference point from which to make future accreditation decisions. Configuration management practices must include periodic reverification of the system configuration to ensure unauthorized changes have not occurred.**

C5.3.6.2.5. Level 4. Complete the Minimal Security Activity Checklist. Analyze the security management procedures' compliance with the approach stated in the SSAA. This analysis must include an examination of the roles and responsibilities assigned to the ISSO to ensure that the responsibilities are consistent with the procedures identified in the SSAA. The system and security management organization must be examined to determine the ability of the ISSO to report security incidents and implement security changes.

C5.3.6.2.5.1. Evaluates the configuration management practices to determine their ability to preserve the integrity of the security relevant software and hardware. A system baseline that identifies all information hardware, software, and firmware components and external interfaces provides for future security evaluations and establishes a known reference point from which to make future accreditation decisions. Configuration management practices must include periodic reverification of the system configuration to ensure unauthorized changes have not occurred.

C5.3.6.2.5.2. **An FCA must be used to demonstrate the readiness of the software for government acceptance testing, as applicable. A PCA must be conducted to check the hardware and software prior to delivery to the**

organization. This check ensures that everything (hardware and software) has been delivered.

C5.3.6.3. Prerequisite Tasks. System integration, Task 2-5 and Task 2-7.

C5.3.6.4. Input. Life-Cycle Management Plan Analysis Summary Report, and Vulnerability Assessment Report.

C5.3.6.5. Output/Products. A System Management Analysis Summary Report must be prepared. This report must include the information shown in Table C5.T2.

C5.3.6.6. Suggested References.

C5.3.6.6.1. "Configuration Management Military Standard" (MIL-STD-973) (reference (ab))

C5.3.6.6.2. "A Guide to Understanding Configuration Management in Trusted Systems" (NCSC-TG-006, Version 1) (reference (ac))

C5.3.6.6.3. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C5.3.6.6.4. "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards" (NIST Special Publication 500-165) (reference (v))

C5.3.6.6.5. "Automated Tools for Testing Computer System Vulnerability" (NIST Special Publication 800-6) (reference (w))

C5.3.7. Task 3-6, Site Accreditation Survey.

C5.3.7.1. Task Objective. The objective of this task is to evaluate the site to ensure that the integration and operation of the system, with its certified design and operational concept, pose an acceptable risk to the information being processed.

C5.3.7.2. Task Description. The site accreditation survey task validates that the site operation of the IS is accomplished as documented in the SSAA. The site accreditation survey analyzes the operational procedures for the IS, environment, personnel security, and physical security to determine if they pose any unacceptable risks to the information being processed. Where the IS is not confined to a fixed site

(tactical or mobile systems and embedded systems in ships or aircraft), the IS must be examined in representative sites or environments.

C5.3.7.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C5.3.7.2.2. Level 2. Complete the Minimal Security Activity Checklist. Conduct a site accreditation survey. This survey must verify that physical, personnel, administrative, and operational security complies with the SSAA and the physical security procedures. The environmental controls (fire sensors, fire suppression, and fire procedures) must be evaluated for consistency with the SSAA and identified for the system architecture.

C5.3.7.2.3. Level 3. Complete the Minimal Security Activity Checklist. Conduct a site accreditation survey. This survey must verify that physical, personnel, administrative, and operational security complies with the SSAA and the physical security procedures. The environmental controls (fire sensors, fire suppression, and fire procedures) must be evaluated for consistency with the SSAA and identified for the system architecture.

C5.3.7.2.4. Level 4. Complete the Minimal Security Activity Checklist. Conduct a site accreditation survey. This survey must verify that physical, personnel, administrative, and operational security complies with the SSAA and the physical security procedures. The environmental controls (fire sensors, fire suppression, and fire procedures) must be evaluated for consistency with the SSAA and identified for the system architecture.

C5.3.7.3. Prerequisite Tasks. Tasks 2-5 and Task 3-1 through Task 3-5.

C5.3.7.4. Input. Site security procedures and practices, Rules of Behavior, Trusted Facility Manual, and Security Features Users Guide.

C5.3.7.5. Output/Products. A Site Accreditation Survey Analysis Summary Report must be prepared that includes the information shown in Table C5.T2.

C5.3.7.6. Suggested References.

C5.3.7.6.1. "Office of Management and Budget Circular No. A-130" (reference (d))

C5.3.7.6.2. "Guideline for Password Usage" (FIPS Publication 112) (reference (aq))

C5.3.7.6.3. "Computer Data Authentication" (FIPS Publication 113) (reference (ar))

C5.3.8. Task 3-7, Contingency Plan Evaluation.

C5.3.8.1. Task Objective. The objective of this task is to ensure that contingency plans are developed and provide reasonable continuity of IS support if events occur that prevent normal operations.

C5.3.8.2. Task Description. The contingency plan evaluation task analyzes the contingency, backup, and continuity of service plans to ensure the plans are consistent with the requirements identified in the SSAA. Periodic testing of the contingency plan is required by DoD Directive 5200.28 (reference (b)) for critical systems and is encouraged for all systems.

C5.3.8.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C5.3.8.2.2. Level 2. Complete the Minimal Security Activity Checklist. Analyze the contingency or continuity of operations plans for completeness to ensure that the plans are consistent with procedures identified in the SSAA. The contingency plans must be evaluated for feasibility. Determine if the contingency plan is periodically tested.

C5.3.8.2.3. Level 3. Complete the Minimal Security Activity Checklist. Analyze the contingency or continuity of operations plans for completeness to ensure that the plans are consistent with procedures identified in the SSAA. The contingency plans must be evaluated for feasibility. Determine if the contingency plan is periodically tested.

C5.3.8.2.4. Level 4. Complete the Minimal Security Activity Checklist. Analyze the contingency or continuity of operations plans for completeness to ensure that the plans are consistent with procedures identified in the SSAA. The contingency plans must be evaluated for feasibility. Determine if the contingency plan is periodically tested.

C5.3.8.3. Prerequisite Tasks. None.

C5.3.8.4. Input. Contingency Plan.

C5.3.8.5. Output/Products. A Contingency Plan Analysis Summary Report

must be prepared. This report must include the information shown in Table C5.T2.

C5.3.8.6. Suggested Reference. "Guidelines for ADP Contingency Planning" (FIPS Publication 87), reference (as)

C5.3.9. Task 3-8, Risk Management Review.

C5.3.9.1. Task Objective. The objective of this task is to assess the overall system security design and architecture against the concept of operations, operational environment, information security policy requirements, and threats to ensure that risks to confidentiality, integrity, availability, and accountability of the information and system are acceptable.

C5.3.9.2. Task Description. The risk management review task assesses the operation of the system to determine if the risk to confidentiality, integrity, availability, and accountability is being maintained at an acceptable level. This review should assess the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures and safeguards should be evaluated to determine their effectiveness and ability to offset risk. The risk management review quantifies the risks the system assets are exposed to in the physical, personnel, administrative, and operating procedures, communications, emanations, hardware, software, and data security areas. A risk is derived from the analysis of a threat and vulnerability to that threat. The purpose of this analysis is to determine if countermeasures are adequate to limit the probability of loss or the impact of loss is reduced to an acceptable level. For each residual risk, a statement should be made to indicate the rationale for accepting or rejecting the risk and possible future modifications to resolve the problem. If future solutions are proposed, a tentative implementation schedule should be included. This is the final review before developing the recommendation to the DAA.

C5.3.9.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C5.3.9.2.2. Level 2. Complete the Minimal Security Activity Checklist. Analyze the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures must be evaluated to determine their ability to offset residual risk. Verify that security Rules of Behavior, a Security Awareness and Training Program, and an Incident Response Program are in place and are current. The Security Awareness Program must provide program and functional managers, end users, IS management, operations and programming staff, and security staff with the tools and procedures required to ensure that the security system is maintained.

C5.3.9.2.3. Level 3. Complete the Minimal Security Activity Checklist. Analyze the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures must be evaluated to determine their ability to offset residual risk. Verify that security Rules of Behavior, a Security Awareness and Training Program, and an Incident Response Program are in place, **are current and effective.** The Security Awareness Program must provide program and functional managers, end users, IS management, operations and programming staff, and security staff with the tools and procedures required to ensure that the security system is maintained.

C5.3.9.2.4. Level 4. Complete the Minimal Security Activity Checklist. Analyze the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures must be evaluated to determine their ability to offset residual risk. Verify that security Rules of Behavior, a Security Awareness and Training Program, and an Incident Response Program are in place, are current and effective. The Security Awareness Program must provide program and functional managers, end users, IS management, operations and programming staff, and security staff with the tools and procedures required to ensure that the security system is maintained. **Conduct tests to verify the effectiveness of the Rules of Behavior and Incident Response Plan.**

C5.3.9.3. Prerequisite Tasks. Tasks 2-7 and Tasks 3-1 through 3-7.

C5.3.9.4. Input. Vulnerability Assessment Report, Threat Analysis, System Design Documentation, PDR and CDR Results, Source Code, IV&V Results.

C5.3.9.5. Output/Products. A Risk Management Analysis Summary Report must be prepared that includes the information shown in Table C5.T2.

C5.3.9.6. Suggested References. None.

C5.4. PHASE 3 ROLES AND RESPONSIBILITIES

C5.4.1. Security Team Responsibilities.

C5.4.1.1. DAA Responsibilities. The DAA must continuously review the system for compliance with the SSAA. During Phase 3 the DAA is responsible for the activities shown in Table C5.T3.

Table C5.T3. DAA Responsibilities

1.	Assess the vulnerabilities and residual risk.
2.	Decide if the security safeguards and residual risk are acceptable.
3.	Approve any corrective actions required.
4.	Sign the accreditation document.

C5.4.1.2. Certifier and Certification Team Responsibilities. During Phase 3, the Certifier and certification team are responsible for the tasks shown in Table C5.T4.

Table C5.T4. Certifier and Certification Team Responsibilities

1.	Complete the Phase 3 certification analysis tasks.
2.	Maintain C&A schedules, plan of action and milestones based on performance of the technical effort.
3.	Integrate changes to the security architecture and system security requirements into the SSAA.
4.	Identify and assess system vulnerabilities.
5.	Recommend risk mitigation measures.
6.	Report certification results to the DAA, program manager, and user representative.
7.	Prepare final SSAA (including all certification evidence).
8.	Provide a recommendation for or against accreditation.

C5.4.2. User Representative Responsibilities. The user representative is responsible for the tasks shown in Table C5.T5. during Phase 3.

Table C5.T5. User Representative Responsibilities

1.	Support certification actions.
2.	Implement and maintain Standard Operating Procedures and Rules of Behavior.
3.	Provide changes to the mission statement, functional environment, and organizational structure to the certification team.
4.	Review certification results.

C5.4.3. Acquisition or Maintenance Organization Responsibilities.

C5.4.3.1. Program Manager Responsibilities. The program manager is responsible for the tasks shown in Table C5.T6. during Phase 3.

Table C5.T6. Program Manager Responsibilities

1.	Support certification team performance of Phase 3 tasks.
2.	Provide access to the IS for the ST&E.
3.	Make system modifications as necessary to reduce or eliminate system vulnerabilities.

C5.4.3.2. Program Management Support Staff Responsibilities. During Phase 3, the program management support staff has the DITSCAP responsibilities shown in Table C5.T7.

Table C5.T7. Program Management Support Staff Responsibilities

1.	Determine the level of effort.
2.	Support the cost and schedule determinations.
3.	Monitor C&A progress.
4.	Maintain system documentation.

C5.4.3.3. Developer, Integrator, or Maintainer Responsibilities. During Phase 3, the developer, integrator, or maintainer is responsible for the tasks shown in Table C5.T8.

Table C5.T8. Developer, Integrator, or Maintainer Responsibilities

1.	Develop or integrate technical security solutions and security requirements.

C5.4.3.4. Configuration Management Responsibilities. During Phase 3, the configuration management staff support the program manager in the development and maintenance of system documentation.

C5.4.3.5. System Administrator Responsibilities. There are no system administration responsibilities in Phase 3.

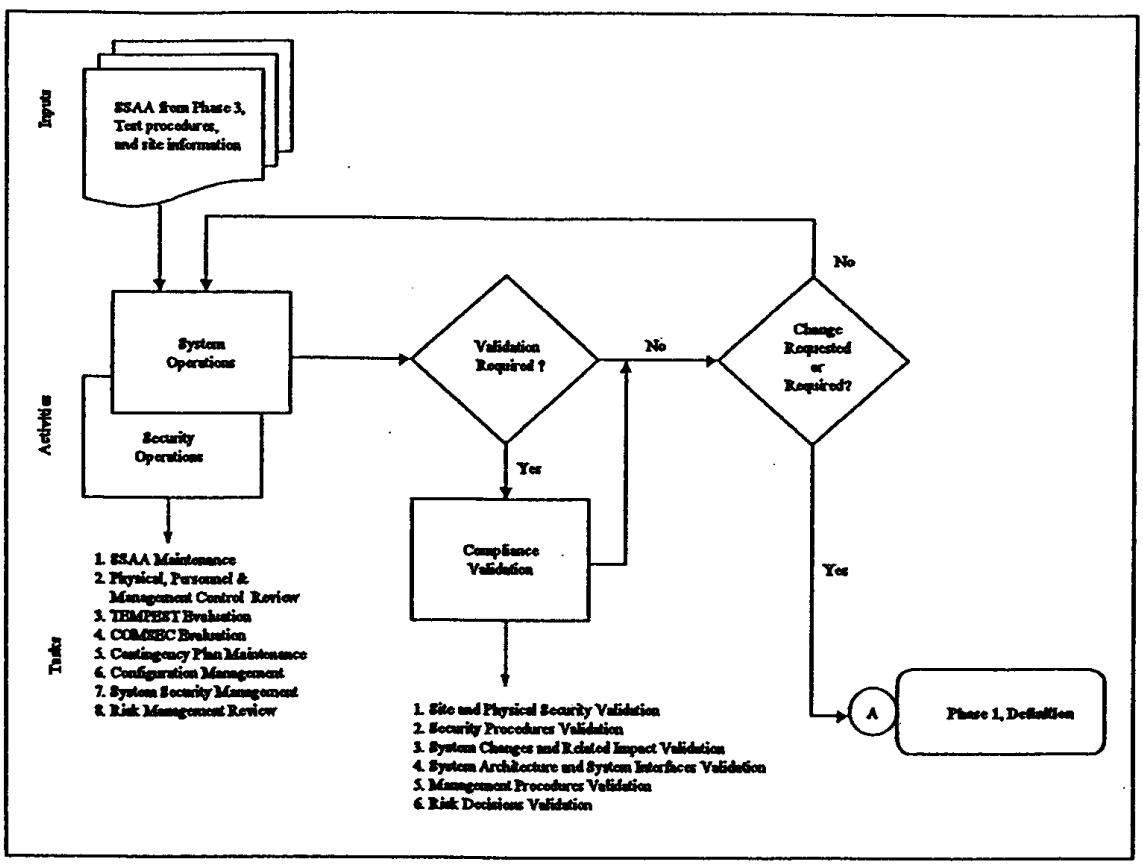
C6. CHAPTER 6

PHASE 4, POST ACCREDITATION

C6.1. PHASE 4 OVERVIEW

C6.1.1. Phase 4 Overview. Phase 4, Figure C6.F1., contains activities required to continue to operate and manage the system so that it will maintain an acceptable level of risk. Post accreditation activities include ongoing maintenance of the SSAA, system operations, security operations, configuration management, and compliance validation.

Figure C6.F1. Post Accreditation Phase



C6.1.2. Phase 4 begins after the system has been integrated into the operational computing environment and accredited. Phase 4 continues until the IS is removed

from service, a major change is planned for the system, or a periodic compliance validation is required. In the first case, the DITSCAP responsibilities of the acquisition organization shift to the system manager or designated maintenance organization. In the other two cases, the DITSCAP reverts to Phase 1. When a major change is planned for a legacy system or the legacy system's periodic validation is required, the DITSCAP process is initiated starting at Phase 1.

C6.2. PHASE 4 ACTIVITIES

C6.2.1. System and Security Operation. The system operation activity include the secure operations of the IS and the associated computing environment. System maintenance tasks ensure that the IS continues to operate within the stated parameters of the accreditation.

C6.2.1.1. Secure system operation depends on the organization and its procedures. Site operations staff and the ISSO are responsible for maintaining an acceptable level of residual risk. That is done by addressing security considerations when changes are made to either the IS baseline or to the baseline of the computing environment operational site. The ISSO is responsible for determining the extent that a change affects the security posture of either the IS or the computing environment, for obtaining approval of security relevant changes, and for documenting the implementation of that change in the SSAA and site operating procedures. Users are responsible for operating the system under the security guidelines established in the SSAA.

C6.2.1.2. Maintaining a security system is an ongoing process that manages risk against the IS, the computing environment, and its resources. Effective management of the risk continuously evaluates the threats that the system is exposed to, evaluates the capabilities of the system and environment to minimize the risk, and balances the security measures against cost and system performance. Secure system management preserves the acceptable level of residual risk based on the relationship of mission, environment, and architecture of the IS and it's computing environment. Secure system management is a continuous review and approval process that involves the users, ISSOs, acquisition or maintenance organizations, and DAA. The Phase 4 security tasks are described in Table C6.T1.

Table C6.T1. System/Security Operations Tasks

1.	SSAA Maintenance
2.	Physical, Personnel, and Management Control Review
3.	TEMPEST Evaluation
4.	COMSEC Compliance Evaluation
5.	Contingency Plan Maintenance
6.	Configuration Management
7.	QSystem Security Management
8.	Risk Management Review

C6.2.2. Compliance Validation. Periodic review of the operational system and its computing environment must occur at predefined intervals, as defined in the SSAA.[11] The purpose of this activity is to ensure the system continues to comply with the security requirements, current threat assessment, and concept of operations. The compliance review should ensure that the contents of the SSAA adequately address the functional environment into which the IS has been placed. The compliance validation tasks should repeat all the applicable Phase 2 and 3 tasks. When compliance validation is conducted, the minimum tasks that should be completed are listed in Table C6.T2.

Table C6.T2. Compliance Validation Tasks

1.	Site and Physical Security Validation
2.	Security Procedures Validation
3.	System Changes and Related Impact Validation
4.	System Architecture and System Interfaces Validation
5.	Management Procedures Validation
6.	Risk Decisions Validation

[11] OMB, DoD, Service, and Agency directives have mandatory recertification and reaccredidation requirements. These requirements must be included in the SSAA, governing security requisites.

C6.3. PHASE 4 CERTIFICATION TASKS

C6.3.1. Phase 4 Task Overview. Phase 4 tasks include both evaluation and maintenance of the secure system operation, site procedures and practices, and environmental requirements unique to the site. The extent of the tasks will depend on the certification level agreed on in the SSAA. After each task is completed, a Task Analysis Summary Report must be prepared. This report must include the information shown in Table C6.T3.

Table C6.T3. Task Analysis Report Topics

1.	Record of findings.
2.	Evaluation of vulnerabilities discovered during evaluations.
3.	Summary of the analysis level of effort.
4.	Summary of tools used and results obtained.
5.	Recommendations.

C6.3.2. Task 4-1, SSAA Maintenance.

C6.3.2.1. Task Objective. The objective of this task is to update the SSAA whenever necessary to ensure it reflects the current operating system mission, environment and architecture.

C6.3.2.2. Task Description. SSAA maintenance is an ongoing task. Each time any change occurs to the system mission, the threat, operating environment, security architecture, or any operating procedures, those changes should be reflected in the SSAA.

C6.3.2.2.1. Level 1. Review the SSAA and make changes as necessary to keep the document and all the attachments current. Submit all security relevant changes to the DAA, program manager, and user representative for approval.

C6.3.2.2.2. Level 2. Review the SSAA and make changes as necessary to keep the document and all the attachments current. Submit all security relevant changes to the DAA, program manager, and user representative for approval.

C6.3.2.2.3. Level 3. Review the SSAA and make changes as necessary to keep the document and all the attachments current. Submit all security relevant changes to the DAA, program manager, and user representative for approval.

C6.3.2.2.4. Level 4. Review the SSAA and make changes as necessary to keep the document and all the attachments current. Submit all security relevant changes to the DAA, program manager, and user representative for approval.

C6.3.2.3. Prerequisite Tasks. All Phase 1, 2, and 3 tasks.

C6.3.2.4. Input. Approved SSAA.

C6.3.2.5. Output/Products. A revised SSAA.

C6.3.2.6. Suggested References. None.

C6.3.3. Task 4-2, Physical, Personnel, and Management Control Review.

C6.3.3.1. Task Objective. The objective of this task is to evaluate the deployment environment of a previously accredited system to ensure compliance with the SSAA.

C6.3.3.2. Task Description. The Phase 3 Site Accreditation Survey task validated that the site operation of the IS was accomplished as documented in the SSAA. This task continues to analyze the operational procedures for the IS, environmental concerns, operational procedures, personnel security controls, and physical security to determine if they pose any unacceptable risks to the information being processed.

C6.3.3.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C6.3.3.2.2. Level 2. Complete the Minimal Security Activity Checklist. Verify that the physical, personnel, environmental, and procedural security complies with the approach stated in the SSAA. This evaluation must determine if the operational environment meets established physical, personnel, environmental controls, and procedural security requirements. When the evaluation has been completed, the results must be documented and included in the SSAA.

C6.3.3.2.3. Level 3. Complete the Minimal Security Activity Checklist. Verify that the physical, personnel, environmental, and procedural security complies with the approach stated in the SSAA. This evaluation must determine if the operational environment meets established physical, personnel, environmental controls, and procedural security requirements. When the evaluation has been completed, the results must be documented and included in the SSAA.

C6.3.3.2.4. Level 4. Complete the Minimal Security Activity Checklist. Verify that the physical, personnel, environmental, and procedural security complies with the approach stated in the SSAA. This evaluation must determine if the operational environment meets established physical, personnel, environmental controls, and procedural security requirements. When the evaluation has been completed, the results must be documented and included in the SSAA.

C6.3.3.3. Prerequisite Tasks. Task 2-5 and Task 3-5 through Task 3-8.

C6.3.3.4. Input. Task Summary Reports from all prerequisite tasks, Site and System Security Operating Procedures.

C6.3.3.5. Output/Products. A Physical, Personnel, and Management Control Review Summary Report summary report must be prepared. This report must include the information shown in Table C6.T3.

C6.3.3.6. Suggested References.

C6.3.3.6.1. "Configuration Management Military Standard" (MIL-STD-973) (reference (ab))

C6.3.3.6.2. "A Guide to Understanding Configuration Management in Trusted Systems" (NCSC-TG-006, Version 1) (reference (ac))

C6.3.3.6.3. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C6.3.4. Task 4-3, TEMPEST Evaluation.

C6.3.4.1. Task Objective. The objective of this task is to validate that the equipment and site continue to meet TEMPEST and RED-BLACK requirements, as appropriate.

C6.3.4.2. Task Description. Periodic TEMPEST and RED-BLACK verification may be required to ensure that the equipment and site meet the security requirements. In these situations the site should be inspected to determine if adequate practices are being followed and the equipment may be subjected to TEMPEST testing.

C6.3.4.2.1. Level 1. Not required.

C6.3.4.2.2. Level 2. Analyze the TEMPEST compliance with the

stated approach in the SSAA. A RED-BLACK facility evaluation must be performed to determine if adequate TEMPEST practices are followed to prevent potential TEMPEST transmissions beyond the PCS. At a minimum, determine that adequate separation exists between RED and BLACK cables, inspect RED power lines for adequate filtering, inspect RED safety grounds and adherence to minimal grounding criteria, examine potential fortuitous conductors for the presence of proper dielectric separators at each PCS or secure area and for the presence of telephone system isolators.

C6.3.4.2.3. Level 3. Analyze the TEMPEST compliance with the approach stated in the SSAA. **Evaluate the site** to determine if adequate TEMPEST practices are followed to reduce potential TEMPEST transmissions beyond the PCS. At a minimum, determine that adequate separation exists between Red and Black cables, inspect Red power lines for adequate filtering, inspect Red safety grounds and adherence to minimal grounding criteria, examine potential fortuitous conductors for the presence of proper dielectric separators at each PCS or secure area and for the presence of telephone system isolators. **Determine the TEMPEST zones for the facility. Inspect the facility and the equipment to determine whether the equipment is placed in the proper zones, or TEMPEST equipment is used if the facility is not zoned.**

C6.3.4.2.4. Level 4. Analyze the TEMPEST compliance with the approach stated in the SSAA. Evaluate the site to determine if adequate TEMPEST practices are followed to reduce potential TEMPEST transmissions beyond the PCS. At a minimum, determine that adequate separation exists between RED and BLACK cables, inspect RED power lines for adequate filtering, inspect RED safety grounds and adherence to minimal grounding criteria, examine potential fortuitous conductors for the presence of proper dielectric separators at each PCS or secure area, and for the presence of telephone system isolators. **By walkaway and conduction tests profile the ERTZ of all RED systems, cables, and components. Ensure that the ERTZ is within the PCS from a three-dimensional perspective.**

C6.3.4.3. Prerequisite Tasks. Task 3-3.

C6.3.4.4. Input. Previously conducted TEMPEST Surveys and Tests, Sensitive Compartmented Information Facility (SCIF) Accreditation Report, Equipment Electrical Operation Specifications, Drawings, and detailed Theory of Operation; Facility Physical Controlled Space Drawings and Equipment Location.

C6.3.4.5. Output/Products. A TEMPEST Evaluation Summary Report must be prepared that includes the information shown in Table C6.T3.

C6.3.4.6. Suggested References.

C6.3.4.6.1. "Laboratory TEMPEST Test Standard" (NSTISSAM TEMPEST/1-92) (reference (ai))

C6.3.4.6.2. "Compromising Emanations Field Test Requirements, Electromagnetics" (NSTISSAM TEMPEST/1-93) (reference (aj))

C6.3.4.6.3. "Procedures for TEMPEST Zoning" (NSTISSAM TEMPEST/2-92) (reference (ak))

C6.3.4.6.4. "Guidelines for Facility Design and Red/Black Installation" (NACSEM 5203) (reference (al))

C6.3.5. Task 4-4, COMSEC Compliance Evaluation.

C6.3.5.1. Task Objective. The objective of this task is to validate that appropriate COMSEC approval has been granted and continues to support the requirements and agreements in the SSAA.

C6.3.5.2. Task Description. This task determines that COMSEC approved key management procedures continue to be used. COMSEC analysis continuously evaluates how well the SSAA defined COMSEC requirements are integrated into the system architecture and the site management procedures.

C6.3.5.2.1. Level 1. Not required.

C6.3.5.2.2. Level 2. Analyze the key management plan to evaluate its compliance with the approach stated in the SSAA. The plan must be evaluated for completeness and compliance with the COMSEC operational and security requirements.

C6.3.5.2.3. Level 3. Analyze the key management **procedures** to evaluate its compliance with the approach stated in the SSAA. The key management plan **and procedures** must be evaluated for completeness and compliance with the COMSEC operational and security requirements. **Analyze the COMSEC modules to evaluate their compliance with the approach stated in the SSAA. The**

COMSEC modules must be evaluated for consistency with the system architecture.

C6.3.5.2.4. Level 4. Analyze the key management procedures to evaluate its compliance with the approach stated in the SSAA. The key management plan and procedures must be evaluated for completeness and compliance with the COMSEC operational and security requirements. The analysis of the COMSEC modules must be evaluated for compliance with the approach stated in the SSAA. **The modules must also be evaluated for consistency with the system architecture and to ensure that cryptographic principles are appropriate for particular applications.**

C6.3.5.3. Prerequisite Tasks. Task 3-4.

C6.3.5.4. Input. Key Management Plan and Procedures, Tailored Functional System Requirements Specifications, embedded COMSEC Modules Design Documentation, previous evaluation of integration of embedded COMSEC modules into the system.

C6.3.5.5. Output/Products. A COMSEC Compliance Evaluation Summary Report must be prepared that includes the information shown in Table C6.T3.

C6.3.5.6. Suggested References.

C6.3.5.6.1. "Communications Security (COMSEC)" (DoD Directive C-5200.5) (reference (am))

C6.3.5.6.2. "Defense Special Security Communications Systems: Security Criteria and Telecommunications Guidance (DoD C-5030.58-M) (reference (an))

C6.3.5.6.3. "Communications Security (COMSEC) Monitoring" (NTISSD 600) (reference (ao))

C6.3.5.6.4. "INFOSEC Software Engineering Standards and Practices Manual" (NSA DS-80) (reference (ap))

C6.3.6. Task 4-5, Contingency Plan Maintenance.

C6.3.6.1. Task Objective. The objective of this task is to ensure that contingency plans are maintained and provide reasonable continuity of IS support when events occur that prevent normal operations.

C6.3.6.2. Task Description. Periodically review the contingency plan and related procedures to ensure they remain current. A contingency plan should cover emergency response, back-up operations, and post-disaster recovery. The plan should consider natural disasters, enemy actions, or malicious attacks. Adequate resources must be available to support the continuity of operations in an emergency situation.

C6.3.6.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C6.3.6.2.2. Level 2. Complete the Minimal Security Activity Checklist. Review contingency plans for the system and site to ensure consistency with the approach stated in the SSAA.

C6.3.6.2.3. Level 3. Complete the Minimal Security Activity Checklist. Review contingency plans for the system and site to ensure consistency with the approach stated in the SSAA.

C6.3.6.2.4. Level 4. Complete the Minimal Security Activity Checklist. Review contingency plans for the system and site to ensure consistency with the approach stated in the SSAA.

C6.3.6.3. Prerequisite Tasks. Task 3-7.

C6.3.6.4. Input. System and Site Contingency Plans, Contingency Plan Analysis Summary Report.

C6.3.6.5. Output/Products. A Contingency Plan Maintenance Summary Report must be prepared that includes the information shown in Table C6.T3.

C6.3.6.6. Suggested Reference. "Guidelines for ADP Contingency Planning" (FIPS Publication 87) (reference (as))

C6.3.7. Task 4-6, Configuration Management.

C6.3.7.1. Task Objective. The objective of this task is to continually assess proposed changes to the system to determine if they will impact the security posture of the accredited system.

C6.3.7.2. Task Description. After an IS is approved for operation in a specific computing environment, changes to the IS and the computing environment must be controlled. While changes may adversely affect the overall security posture of the infrastructure and the IS, change is ongoing as it responds to the needs of the

user and new technology developments. As the threats become more sophisticated or focused on a particular asset, countermeasures must be strengthened or added to provide adequate protection. Therefore, configuration management is required to maintain an acceptable level of residual risk.

C6.3.7.2.1. Accreditation is based on security assumptions that tie certified hardware and software of each system to the configuration of the computing environment. Changes in the IS configuration, operational mission, computing environment, or to the computing environment's configuration may invalidate the security assumptions.

C6.3.7.2.2. The program manager, ISSO, and system users must support the system configuration management process. They must be involved in the configuration management process to ensure that changes do not have an adverse affect on the security posture of the system and its associated IS. The strategy for managing change must be defined in the SSAA. The ISSO must review and approve changes relating to security and document the implementation of a change in the SSAA. Changes that significantly affect the system security posture must be forwarded to the DAA, Certifier, user representative, and program manager.

C6.3.7.2.3. Level 1. Review the proposed system changes to determine if they have any impact on the system security posture.

C6.3.7.2.4. Level 2. Attend the configuration management review board meetings (or their equivalent) and review each proposed system change before they are implemented. **Monitor the system for events that may indicate that the system needs to be recertificed. These events may include changes to security critical software or hardware, changes to the threat, changes in the mission, or unauthorized system changes. Update the SSAA as appropriate.**

C6.3.7.2.5. Level 3. Attend the configuration management review board meetings (or their equivalent) and review each proposed system change before they are implemented. Monitor the system for events that may indicate that the system needs to be recertificed. These events may include changes to security critical software or hardware, changes to the threat, changes in the mission, or unauthorized system changes. **Test the system with automated tools to verify that the system configuration has not changed. Update the SSAA as appropriate.**

C6.3.7.2.6. Level 4. Attend the configuration management review board meetings (or their equivalent) and review each proposed system change before

they are implemented. Monitor the system for events that may indicate that the system needs to be recertificed. These events may include changes to security critical software or hardware, changes to the threat, changes in the mission, or unauthorized system changes. Test the system with automated tools to verify that the system configuration has not changed. Update the SSAA as appropriate.

C6.3.7.3. Prerequisite Tasks. Task 2-5, Task 3-5, and Task 4-1.

C6.3.7.4. Input. Current SSAA, System Design Documentation, PDR and CDR results, Source Code, Configuration Management Review Board minutes and notes, System Change Requests.

C6.3.7.5. Output/Products. A Configuration Management Summary Report must be prepared. This report must include the information shown in Table C6.T3.

C6.3.7.6. Suggested Reference. "Configuration Management Military Standard" (MIL-STD-973) (reference (ab))

C6.3.8. Task 4-7, Risk Management Review.

C6.3.8.1. Task Objective. The objective of this task is to assess the overall system security design, architecture, and other SSAA requirements against the concept of operations, operational environment, and threats to ensure that risk to confidentiality, integrity, availability, or accountability of the information and system remains acceptable. Known threats, as well as any new threats, must be analyzed to determine if the system still adequately protects against all them. Possible threat changes include those items shown in Table C6.T4.

Table C6.T4. Possible Threat Changes

1.	A change in the IT mission or user profile.
2.	A change in the IT architecture, such as the addition of a LAN or WAN connection.
3.	A change in criticality and/or sensitivity level that causes a change in the countermeasures required.
4.	A change in the security policy.
5.	A change in the threat or system risk.
6.	A change in the activity that requires a different security mode of operation.
7.	A breach of security, a breach of system integrity, or an unusual situation that may invalidate the accreditation by revealing a flaw in security design.
8.	Results of an audit or external assessment.

C6.3.8.2. Task Description. The risk management review task continues to assess the operation of the system to determine if the risk to confidentiality, integrity, availability, and accountability is being maintained at an acceptable level. This review should assess the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures and safeguards should be evaluated to determine their effectiveness and ability to offset risk. Any changes to the risk should immediately be reported to the DAA.

C6.3.8.2.1. Level 1. Complete the Minimal Security Activity Checklist.

C6.3.8.2.2. Level 2. Complete the Minimal Security Activity Checklist. Analyze the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures must be evaluated to determine their ability to offset residual risk. Verify that security Rules of Behavior, a Security Awareness and Training Program and an Incident Response Program are in place and are current. The Security Awareness Program must provide program and functional managers, end users, IS management, operations and programming staff, and security staff with the tools and procedures required to ensure that the security system is maintained. Evaluate the availability and effectiveness of tools and procedures to ensure that the security system is maintained.

C6.3.8.2.3. Level 3. Complete the Minimal Security Activity Checklist. Analyze the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures must be evaluated to determine their ability to offset residual risk. Verify that security Rules of Behavior, a Security Awareness and Training Program and an Incident Response Program are in place, **are current, and are effective.** The Security Awareness Program must provide program and functional managers, end users, IS management, operations and programming staff, and security staff with the tools and procedures required to ensure that the security system is maintained. Evaluate the availability and effectiveness of tools and procedures to ensure that the security system is maintained. **Capabilities of the tools may include real-time monitoring and alerts, intrusion detection, network analysis, audit analysis, user management, risk analysis, and network configuration management tools.**

C6.3.8.2.4. Level 4. Complete the Minimal Security Activity Checklist. Analyze the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational

procedures must be evaluated to determine their ability to offset residual risk. Verify that security Rules of Behavior, a Security Awareness and Training Program and an Incident Response Program are in place are current, and are effective. The Security Awareness Program must provide program and functional managers, end users, IS management, operations and programming staff, and security staff with the tools and procedures required to ensure that the security system is maintained. **Conduct tests to verify the effectiveness of the Rules of Behavior and Incident Response Plan.** Evaluate the availability and effectiveness of tools and procedures to ensure that the security system is maintained. Capabilities of the tools may include real-time monitoring and alerts, intrusion detection, network analysis, audit analysis, user management, risk analysis, and network configuration management tools.

C6.3.8.3. Prerequisite Tasks. Task 2-6, Task 3-6 through Task 3-8, and Task 4-1 through Task 4-6.

C6.3.8.4. Input. SSAA, Risk Analysis, Threat Analysis, Vulnerability Evaluation, and IV&V results, Task Summary Reports from all prerequisite tasks.

C6.3.8.5. Output/Products. An updated SSAA and a Risk Management Review Summary Report must be prepared. This report must include the information shown in Table C6.T3.

C6.3.8.6. Suggested References.

C6.3.8.6.1. "Guideline for Life-Cycle Validation, Verification, and Testing of Computer Software" (FIPS Publication 101) (reference (u))

C6.3.8.6.2. "Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards" (NIST Special Publication 500-165) (reference (v))

C6.3.8.6.3. "Automated Tools for Testing Computer System Vulnerability" (NIST Special Publication 800-6) (reference (w))

C6.3.8.6.4. "Systems Engineering Management Guide" (Defense Systems Management College, January 1990) (reference (n))

C6.3.8.6.5. "A Guide to Understanding Audit in Trusted Systems" (NCSC-TG-001, Version 2) (reference (x))

C6.3.8.6.6. "A Guide to Understanding Discretionary Access Control in Trusted Systems" (NCSC-TG-003, Version 1) (reference (y))

C6.3.8.6.7. "A Guide to Understanding Configuration Management in Trusted Systems" (NCSC-TG-006, Version 1) (reference (ac))

C6.3.8.6.8. "A Guide to Understanding Design Documentation in Trusted Systems" (NCSC-TG-021, Version 1) (reference (r))

C6.3.8.6.9. "A Guide to Understanding Trusted Distribution in Trusted Systems" (NCSC-TG-008, Version 1) (reference (ad))

C6.3.8.6.10. "Trusted Network Interpretation Environments Guideline" (NCSC-TG-011, Version 1) (reference (s))

C6.3.8.6.11. "Rating Maintenance Phase Program Documentation" (NCSC-TG-013) (reference (ae))

C6.3.8.6.12. "A Guide to Understanding Trusted Facility Management" (NCSC-TG-015, Version 1) (reference (af))

C6.3.8.6.13. "A Guide to Understanding Identification and Authentication in Trusted Systems" (NCSC-TG-017, Version 1) (reference (z))

C6.3.8.6.14. "A Guide to Understanding Object Reuse in Trusted Systems" (NCSC-TG-018, Version 1) (reference (aa))

C6.3.8.6.15. "Trusted Database Management System Interpretation" (NCSC-TG-012) (reference (p))

C6.3.8.6.16. "A Guide to Understanding Trusted Recovery in Trusted Systems" (NCSC-TF-022) (reference (t))

C6.3.8.6.17. "Assessing Controlled Access Protection" (NCSC-TG-028) (reference (q))

C6.3.9. Task 4-8, Compliance Validation.

C6.3.9.1. Task Objective. The objective of the compliance validation tasks are to ensure that the IS complies with the security requirements, current threat assessment, and concept of operations.

C6.3.9.2. Task Description. The compliance validation tasks ensure that the contents of the SSAA adequately address the functional environment into which the IS has been placed. The compliance validation tasks should repeat all the applicable Phase 2 and 3 tasks. At a minimum, when compliance validation is conducted, the minimum tasks that should be conducted are listed in Table C6.T5.

Table C6.T5. Compliance Validation Tasks

1.	Site and Physical Security Validation
2.	Security Procedures Validation
3.	System Changes and Related Impact Validation
4.	System Architecture and System Interfaces Validation
5.	Management Procedures Validation
6.	Risk Decisions Validation

C6.3.9.2.1. Level 1. Complete the Minimum Security Activity Checklist.

C.6.3.9.2.2. Level 2. Conduct the appropriate activities from Phase 2 and 3 tasks to adequately validate the system compliance within its operating environment.

C6.3.9.2.3. Level 3. Conduct the appropriate activities from Phase 2 and 3 tasks to adequately validate the system compliance within its operating environment.

C6.3.9.2.4. Level 4. Conduct the appropriate activities from Phase 2 and 3 tasks to adequately validate the system compliance within its operating environment.

C6.3.9.3. Prerequisite Tasks. All Phase 2 and 3 tasks.

C6.3.9.4. Input. Approved SSAA, Task Summary Reports from all prerequisite tasks.

C6.3.9.5. Output/Products. A Compliance Validation Summary Report must be prepared. This report must include the information shown in Table C6.T3.

C6.3.9.6. Suggested References.

C6.3.9.6.1. See references from related Phase 2 and 3 tasks.

C6.4. PHASE 4 ROLES AND RESPONSIBILITIES

C6.4.1 Security Team Responsibilities.

C6.4.1.1. DAA Responsibilities. The DAA must continuously review the system for compliance with the SSAA. During Phase 4, the DAA is responsible for the tasks shown in Table C6.T6.

Table C6.T6. DAA Responsibilities

1.	Review proposed security changes.
2.	Oversee compliance validation.
3.	Monitor C&A integrity.
4.	Establish reaccredidation requirements and ensuring all assigned systems comply with these requirements.
5.	Decide to reaccreditate, accredit, IATO, or if the SSAA is no longer valid, terminate system operations.

C6.4.1.2. Certifier and Certification Team Responsibilities. The Certifier and certification team normally are not involved with the system in Phase 4. Their roles and responsibilities in Phase 4 are to support of the DAA, system operators, and ISSO as mutually agreed.

C6.4.2. User Responsibilities.

C6.4.2.1. User Representative Responsibilities. During Phase 4, the user representative has the responsibilities shown in Table C6.T7.

Table C6.T7. User Representative Responsibilities

1.	Oversee the system operation according to the SSAA.
2.	Report vulnerability and security incidents.
3.	Report threats to the mission environment.
4.	Review and update the system vulnerabilities.
5.	Review changes to the security policy and standards.
6.	Initiate SSAA review if there are changes in the threat or system configuration.

C6.4.2.2. ISSO Responsibilities. The ISSO is usually the security focal point within the user community, responsible for the secure operation of the IS within the environment agreed on in the SSAA. The ISSO ensures the IS is deployed and operated according to the SSAA through integration of all the security disciplines

(COMPUSEC, COMSEC, EMSEC, personnel, physical, and administrative procedures) to maintain an acceptable level of residual risk. The responsibilities of the ISSO during Phase 4 include those shown in Table C6.T8.

Table C6.T8. ISSO Responsibilities

1.	Periodically review the mission statement, operating environment, and security architecture to determine compliance with the approved SSAA.
2.	Maintain the integrity of the site environment and accredited security posture.
3.	Ensure that configuration management adheres to the security policy and security requirements.
4.	Initiate the C&A process when periodic reaccredidation is required or system change dictates.

C6.4.3. Acquisition or Maintenance Organization Responsibilities.

C6.4.3.1. Program Manager Responsibilities. The development program manager role shifts to the system operator in Phase 4. During Phase 4, the program manager responsibilities are performed by the owner or operator of the IS, as shown in Table C6.T9.

Table C6.T9. Program Manager Responsibilities

1.	Report security related changes in the IS to the DAA and user representative.
2.	Update the IS to address reported vulnerabilities and patches under configuration management.
3.	Review and update life-cycle management policies and standards.
4.	Resolve security discrepancies.

C6.4.3.2. Program Management Support Staff Responsibilities. During Phase 4, the program management support staff is responsible for cost and schedule determinations, level of effort evaluation of subsequent C&A efforts, and system documentation.

C6.4.3.3. Developer, Integrator, or Maintainer Responsibilities. During Phase 4, the developer/integrator responsibilities normally shift to the organization responsible for the system maintenance. The Phase 4 responsibilities are shown in Table C6.T10.

Table C6.T10. Developer, Integrator or Maintainer Responsibilities

1.	Provide hardware and software architecture to the acquisition organization.
2.	Provide system modifications or changes to the ISSO and informing the program manager, DAA, Certifier, and user representative.
3.	Develop or integrate technical security solutions and security requirements.

C6.4.3.4. Configuration Control and Configuration Management Responsibilities. During Phase 4, the configuration control and configuration management staff supports the PM in the development and maintenance of system documentation.

C6.4.3.5. System Administration Responsibilities. During Phase 4, system administration responsibilities include the tasks shown in Table C6.T11.

Table C6.T11. System Administrator Responsibilities

1.	Operate the system according to the SSAA.
2.	Maintain an acceptable level of residual risk.
3.	Inform the ISSO of any proposed changes or modifications to the system, information processed, operating procedures, operating environment that affect security.

C7. CHAPTER 7

SECURITY ACTIVITIES IN THE SYSTEM LIFE CYCLE

C7.1. OVERVIEW

DoD Directive 5000.1 (reference (h)) and DoD 5000.2-R, reference (i), describe the phases and milestones for the design, development, deployment, operation, support, and/or termination and disposal of major automated IS. The security activities and conditions to initiate and complete each phase and milestone are defined in the sections below.

C7.2. IS PROGRAM STRATEGIES

C7.2.1. A program strategy is the method used to design, develop, and deploy an IS through its life cycle. Four general program strategies have been used; grand design, incremental, evolutionary, and other.

C7.2.1.1. Grand Design Program Strategies. Acquisition, development, and deployment of the total functional capability in a single increment characterize the grand design program strategies. The required functional capability can be defined clearly, and further enhancement is not foreseen to be necessary. A grand design program strategy usually is used when the user requirements are well understood, supported by precedent, easily defined, and assessment of other considerations (risks, funding, schedule, size of program, or early realization of benefits) indicates that a phased approach is not required.

C7.2.1.2. Incremental Program Strategies. Acquisition, development, and deployment of functionality through a number of clearly defined system increments that stand on their own characterize incremental program strategies. The number, size, and phasing of the increments required for satisfaction of the total scope of the stated user requirement will be defined by the IS program manager, in consultation with the functional user. An incremental program strategy usually is used when the user requirements are well understood and easily defined, but assessment of other considerations (risks, funding, schedule, size of the program, or early realization of benefits) indicates that a phased approach is more prudent or beneficial.

C7.2.1.3. Evolutionary Program Strategies. Evolutionary program strategies are characterized by the design, development, and deployment of a preliminary capability that includes provisions for the evolutionary addition of future functionality and changes as requirements are further defined. Evolutionary developments are conducted within the context of a plan for evolution towards an ultimate capability. The total functional requirements the IS must meet are refined successively through feedback from previous increments and reflected in subsequent increments. Evolutionary program strategies are particularly suited to situations where, although the general scope of the program is known and a basic core of user functional characteristics can be defined, detailed system or functional requirements are difficult to articulate (decision-aiding systems requiring extensive human-machine interaction). The evolutionary program strategy differs from the incremental program strategy because the total functional capability is not completely defined at inception, but evolves as the system is built.

C7.2.1.4. Other Program Strategies. Other program strategies are intended to encompass variations and/or combinations of the program strategies in the previous subparagraphs, or other program strategies not listed above (OMB Circular A-109 acquisitions (reference (av)), COTS, NDI, and commercial item acquisitions).

C7.3. IS LIFE-CYCLE MANAGEMENT PROCESS

C7.3.1. An overview of the tasks applicable to each Life-Cycle Management (LCM) phase and the decision process for each milestone are described in the next sections. Those tasks are essentially the same for all program strategies before Milestone I. Subsequent tasks must be tailored to the program strategy approved at Milestone I. The proposed program strategy must be outlined during the Concept Exploration and Definition phase (Phase 0) and approved at Milestone I.

C7.3.1.1. Rapid prototyping may be used throughout the LCM process. It may be used to support analysis performed during the Concept Exploration and Definition and Demonstration and Validation phases. Additionally, rapid prototyping may be used to develop a subset of functionality in whichever program strategy is selected.

C7.3.1.2. Depending on the selected program strategy, combined or repeated milestone decision points and associated activities within the user representative phase may be required. The number of replicated decision points and how increments between those decision points are to be reviewed will be specified in the proposed

program strategy presented at Milestone I. For example, in an evolutionary program strategy, there may be multiple Milestone II and Milestone III decision points, depending on the amount of functionality provided in each increment. Replicated milestone decision point implies repeating the phases preceding the milestone decision point. A second example is that the use of GOTS, COTS, and/or NDI products, requiring no custom changes, may result in the consolidation of the LCM Demonstration and Validation and the Development phases. In that case, a combined Milestone II and III review is justified. Similar tailoring may be applicable to migration systems.

C7.3.1.3. At each milestone decision point, the status of program execution and plans for the next phase and the remainder of the program must be assessed. The risks associated with that program and the adequacy of risk management planning must be addressed explicitly. Additionally, program-specific results to be required in the next phase, called "exit criteria," must be established. Exit criteria are critical results that must be attained during the next phase. They can be viewed as gates through which a program must pass during that phase. For example, they can include the requirement to achieve a specified level of performance in testing, or conduct a critical design review before committing funds for future procurement.

C7.3.2. Milestones and Phases.

C7.3.2.1. Milestone 0 - Approval to Conduct Concept Studies. After the mission need is validated, a Milestone 0 review is conducted to review the mission needs statement, identify possible alternatives, and authorize concept studies.

C7.3.2.2. Phase 0 - Concept Exploration. Phase 0 typically consists of competitive, parallel short-term concept studies. The focus of these efforts is to define and evaluate the feasibility of alternative concepts and to provide a basis for assessing the relative merits of these concepts at the next milestone decision point.

C7.3.2.3. Milestone I - Approval to Begin a New Acquisition Program. The purpose of the Milestone I decision point is to determine if the results of Phase 0 warrant establishing a new acquisition program and to approve entry into Phase I.

C7.3.2.4. Phase I, Program Definition and Risk Reduction. During this phase the program must become defined as one or more concepts, design approaches, and/or parallel technologies are pursued as warranted. Assessments of the advantages and disadvantages of alternative concepts must be refined. Prototyping, demonstrations, and early operational assessments must be considered and included as necessary to reduce risk and ensure that technology, manufacturing, and support risks

are well in hand before the next decision point. Cost-drivers, life-cycle cost estimates, cost-performance trades, interoperability, and acquisition strategy alternatives must be considered to include evolutionary and incremental software development. The activities of this phase will depend on the approved program strategy, Table C7.T1.

Table C7.T1. Phase I Activities by Program Strategy

1.	Grand Design. Validate the selected system design and complete the technical specifications.
2.	Incremental. Design, code, test, and demonstrate a subset of functional capabilities to support the program strategy.
3.	Evolutionary. Design, code, test, and demonstrate a program that provides basic or elementary capabilities in the context of a plan for evolution towards an ultimate capability.
4.	Other. The activities to be accomplished during this phase will depend on the specific definition of the program strategy.

C7.3.2.5. Milestone II - Approval to Enter Engineering and Manufacturing. The purpose of Milestone II is to determine if the results of Phase I warrant continuation of the program and to approve entry into Engineering and Manufacturing Development (or software engineering and development for a software intensive system).

C7.3.2.6. Phase II - Engineering and Manufacturing Development. The primary objectives of this phase are to translate the most promising design approach into a stable, interoperable, producible, supportable, and cost-effective design; validate the manufacturing or production process; and to demonstrate system capabilities through testing. The activities of this phase, Table C7.T2., will depend on the approved program strategy.

Table C7.T2. Phase II Activities by Program Strategy

1.	Grand Design. Develop the IS, test it when complete to ensure that it satisfies mission needs described in the mission needs statement and prepare for deployment.
2.	Incremental. The activities in this phase may be repeated. For each recurrence of the phase, code, and test the applicable increments of the overall design. Ensure that all capabilities to which the user agreed are satisfied. Prepare for deployment.
3.	Evolutionary. The activities in this phase may be repeated. For each recurrence of the phase, design, code, and test the applicable increments as they progress toward an overall design. Ensure that all user agreements are satisfied. Prepare for deployment.
4.	Other. The activities to be accomplished during this phase will depend on the specific definition of the program strategy.

C7.3.2.7. Milestone III - Production or Fielding/Deployment Approval. The purpose of Milestone III is to authorize entrance into production for an ACAT I or into deployment for an ACAT IA program.

C7.3.2.8. Phase III - Production, Fielding/Deployment, and Operational Support. The objectives of this phase are to achieve an operational capability that satisfies the mission needs. Deficiencies encountered in the Developmental Test and Evaluation (DT&E) and Initial Operational Test and Evaluation (IOT&E) must be resolved and fixes verified. During the fielding/deployment and throughout operational support, the potential for modifications to the fielded/deployed system continues.

C7.3.2.8.1. Operational Support. The objectives of this activity are the execution of a support program that meets the threshold values of all support performance requirements and sustainment of them in the most life-cycle cost-effective manner.

C7.3.2.8.2. Modifications. Any modification that is of sufficient cost and complexity that it could itself qualify as an ACAT I or ACAT IA program must be considered for management purposes as a separate acquisition effort. Modifications that do not cross the ACAT I or IA threshold must be considered part of the program being modified. Modifications may cause a baseline deviation. In either of these cases a new DITSCAP process must be initiated.

C8. CHAPTER 8

DITSCAP MANAGEMENT

C8.1. MANAGEMENT OVERVIEW

C8.1.1. Many organizations within the Department of Defense have significant roles in contributing to the secure development and operation of the IS. [12] The DITSCAP approach allows the Services or Agencies to adapt the DITSCAP roles into their respective organizational management structure to best manage the risks to their mission throughout the IS life cycle: system development, operation, maintenance, and disposal.

C8.1.2. The DITSCAP management approach integrates existing C&A roles at multiple levels; first at the Service or Agency level, then at the site and system levels. At the Service or Agency level, the process should be tailored to the organization's specific needs and management approach. At the site and system levels, the process should be tailored to implement Service or Agency requirements and to meet the needs of the specific system and the risks associated with operating that system.

C8.2. DITSCAP ROLES AND RESPONSIBILITIES

C8.2.1. The key roles in the DITSCAP are the program manager, DAA, Certifier, and user representative. Additional roles may be added to increase the integrity and objectivity of C&A decisions in support of the system business case or mission. For example, the ISSO usually performs a key role in the maintenance of the security posture after accreditation.

C8.2.1.1. Program Manager. The program manager represents the interests of the system throughout its life cycle (acquisition or maintenance, life-cycle schedules, funding responsibilities, system operations, performance, and maintenance). The organization the program manager represents is determined by the phase in the life cycle of the system.

---

[12] Only users with .mil or .gov accounts are permitted to access the IASE.

C8.2.1.2. DAA. The DAA is usually a senior operational commander with the authority and ability to evaluate the mission, business case, and budgetary needs for the system in view of the security risks. The DAA must have the authority to oversee the budget and IS operations of systems under his/her purview. The DAA determines the acceptable level of residual risk and approves the system operation.

C8.2.1.3. Certifier. The Certifier (and certification team) provides the technical expertise to conduct the certification through the system's life cycle based on the security requirements documented in the SSAA. The Certifier determines the level of residual risk and makes an accreditation recommendation to the DAA.

C8.2.1.4. User Representative. The operational interests of the systems users are vested in the user representative. In the DITSCAP process, the user representative is concerned with system availability, access, integrity, functionality, and performance in addition to confidentiality as they relate to the system mission.

C8.2.1.5. The DITSCAP allows these individuals to tailor and scope the C&A efforts to the particular mission, environment, system architecture, threats, funding, and schedule of the system. Table C8.T1. summarizes the DITSCAP roles and responsibilities.

Table C8.T1. Management Responsibilities by DITSCAP Phase

Phase	Mgmt. Roles	Security Roles		User Roles
	Program Manager	**DAA**	**Certifier**	**User Rep.**
Phase 1	• Initiate security dialogue with DAA, Certifier, and user representative • Define system schedule and budget • Support DITSCAP tailoring and level of effort determination • Define system architecture Prepare Life-Cycle Management Plans • Define security architecture	• Define accreditation requirements • Obtain threat assessment • Assign the Certifier Support DITSCAP tailoring • Approve the SSAA	• Begin vulnerability and risk assessments • Review threat definition • Lead DITSCAP tailoring • Determine level of certification effort • Describe certification team roles and responsibilities • Draft SSAA	• Support DITSCAP tailoring and level of effort determination • Define operational needs in terms of mission • Identify vulnerabilities to mission • Define operational resource constraints
Phase 2	• Develop system or system modifications • Support certification activities • Review certification results • Revise system as needed • Resolve security discrepancies	• Support certification activities	• Conduct certification activities • Assess vulnerabilities • Report results to the program manager, DAA, and user representative • Determine if system is ready for certification • Update the SSAA	• Prepare security Rules of Behavior (ROB) and Standard Operating Procedures (SOP) • Support certification actions

Table C8.T1. Management Responsibilities by DITSCAP Phase--Continued

Phase	Mgmt. Roles	Security Roles		User Roles
	Program Manager	**DAA**	**Certifier**	**User Rep.**
Phase 3	• Support certification activities • Provide IS access for ST&E • Provide system corrections under configuration management	• Assess vulnerabilities and residual risk • Decide to accredit, IATO, or terminate system operations	• Conduct certification activities • Evaluate security requirements compliance • Assess vulnerabilities and residual risk • Report results to the program manager, DAA, and user representative • Recommend risk mitigation measures • Prepare final SSAA • Recommend accreditation type	• Support certification efforts • Implement and maintain SOP and ROB • Review certification results
Phase 4	• Update IS to address Phase 3 reported vulnerabilities and patches under configuration management • Report security related changes to the IS to the DAA and user representative • Review and update life-cycle management policies and standards • Resolve security discrepancies	• Review the SSAA • Review proposed changes • Oversee compliance validation • Monitor C&A integrity • Decide to reaccredit, accredit, IATO, or, if SSAA is no longer valid, terminate system operations		• Report vulnerability and security incidents • Report threats to mission environment • Review and update system vulnerabilities • Review and change security policy and standards • Initiate SSAA review if changes to threat or system

C8.3. PROGRAM MANAGER

C8.3.1. The program manager coordinates all aspects of the system from initial concept, through development, to implementation and system maintenance. The DAA, Certifier, and user representative provide advise, information, and guidance to the program manager throughout the DITSCAP process.

C8.3.2. The program manager is responsible for the IS throughout the life cycle (cost, schedule, and performance of the system development). The program manager's function in the DITSCAP is to ensure that the security requirements are integrated in a

way that will result in an acceptable level of risk to the operational infrastructure as documented in the SSAA. The program manager keeps all DITSCAP participants informed of life-cycle actions, security requirements, and documented user needs.

C8.3.3. During Phase 2, the program manager provides details of the system and its life-cycle management to the DAA, Certifier, and user representative. The program manager must verify that the implementation of the system is consistent with the system security characteristics reflected in the SSAA. As additional system details become available, the program manager ensures the SSAA is updated. At the end of Phase 2, the program manager ensures a configuration management procedure is in place and the system is properly controlled during the certification process.

C8.3.4. During Phase 3, the program manager ensures that the certification ready system is under configuration management. The DAA, Certifier, and user representative validate that the operational environment and system configuration is consistent with the security characteristics reflected in the SSAA.

C8.4. DAA

C8.4.1. The DAA is the primary Government official responsible for system security. Based on national, Agency, and organizational policies and guidance, and input from the user representative and program manager, the DAA directs the security activities of the Certifier and ISSO.

C8.4.2. The DAA is the official responsible for accepting a level of risk for the operation of the IS. Based on the information available in the SSAA, the DAA can grant an accreditation, IATO, or may determine that the system's risks are not at an acceptable level and is not ready to be operational. In reaching these decisions, the DAA is supported by all the documentation provided in the SSAA.

C8.4.3. The IS may involve multiple DAAs. If so, an agreement must be established among the DAAs. The agreement is an integral portion of the SSAA. In most cases, it will be advantageous to agree to a lead DAA to represent the DAAs involved in the system.

C8.5. CERTIFIER

The Certifier determines whether a system is ready for certification and conducts the certification process; a comprehensive evaluation of the technical and non-technical

security features of the system. At the completion of the certification effort, the Certifier reports the status of certification and recommends to the DAA whether or not to accredit the system based on documented residual risk. The Certifier should be independent from the organization responsible for the system development or operation. Organizational independence of the Certifier ensures the most objective information for the DAA to make accreditation decisions.

C8.6. ISSO

The ISSO is responsible for administering the security requirements for an IS during its operation. Within the user community, the ISSO is responsible for monitoring the secure operation of the IS within the environment defined in the SSAA. The ISSO ensures the IS is deployed and operated according to the security requirements documented in the SSAA through integration of all the security disciplines (computer security, communication security, information security, emissions security, personnel, physical, and administrative procedures) to maintain an acceptable level of residual risk. Since operational scenarios within DoD Services and Agencies vary, the exact location and number of ISSO(s) within a single Agency may be different. The organization may appoint a single ISSO to coordinate the actions of an IS at multiple sites or environments or appoint an ISSO for each system, site, or environment. User organizations should assign the ISSOs to an organizational position where the ISSO has direct access to the appropriate decision makers.

C8.7. USER REPRESENTATIVE

The users are responsible for the identification of operational requirements and the secure operation of a certified and accredited IS, based on the SSAA. The user representative represents the user community and assists in the C&A process. The user representative is the liaison for the user community throughout the life cycle of the system. The user representative defines the system's operations and functional requirements and is responsible for ensuring that the user's operational interests are maintained throughout system development, modification, integration, acquisition, and deployment.

AP1. APPENDIX 1

SSAA OUTLINE AND DETAILED DESCRIPTION

AP1.1. SSAA OUTLINE

AP1.1.1. Document. The SSAA is a living document that represents the formal agreement between the DAA, CA, program manager, and user representative. The SSAA is developed in Phase 1 and updated in each phase as the system development progresses and new information becomes available. At a minimum, the SSAA should contain the information in the following sample outline:

1.0. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

1.1. System Name and Identification

1.2. System Description

1.3. Functional Description

1.3.1. System Capabilities

1.3.2. System Criticality

1.3.3. Classification and Sensitivity of Data Processed

1.3.4. System User Description and Clearance Levels

1.3.5. Life Cycle of the System

1.4. System CONOPS Summary

2.0. ENVIRONMENT DESCRIPTION

2.1. Operating Environment

2.1.1. Facility Description

2.1.2. Physical Security

2.1.3. Administrative Issues

5.0. ORGANIZATIONS AND RESOURCES

5.1. Organizations

5.2. Resources

5.3. Training

5.4. Other Supporting Organizations

6.0. DITSCAP PLAN

6.1. Tailoring Factors

6.1.1. Programmatic Considerations

6.1.2. Security Environment

6.1.3. IS Characteristics

6.1.4. Reuse of Previously Approved Solutions

6.2. Tasks and Milestones

6.3. Schedule Summary

6.4. Level of Effort

6.5. Roles and Responsibilities

AP1.1.2 Appendices. Appendices should include system C&A artifacts. Optional appendices may be added to meet specific needs. Include all documentation that is relevant to the C&A process.

Appendix A Acronyms

Appendix B Definitions

Appendix C References

Appendix D System Concept of Operations

Appendix E Information System Security Policy

Appendix F Security Requirements and/or Requirements Traceability Matrix

Appendix G Certification Test and Evaluation Plan and Procedures (Type only)

Appendix H Security Test and Evaluation Plan and Procedures

Appendix I Applicable System Development Artifacts or System Documentation

Appendix J System Rules of Behavior

Appendix K Incident Response Plan

Appendix L Contingency Plans

Appendix M Personnel Controls and Technical Security Controls

Appendix N Memorandums of Agreement – System Interconnect Agreements

Appendix O Security Education, Training, and Awareness Plan

Appendix P Test and Evaluation Report(s)

Appendix Q Residual Risk Assessment Results

Appendix R Certification and Accreditation Statement

AP2. APPENDIX 2

MINIMAL SECURITY ACTIVITY CHECKLIST

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

System Architecture Analysis	YES	NO	N/A
1. Does the systems architecture documentation describe the architecture, including graphics, of the system and interconnections providing or supporting, system functions?			
2. For a domain, does the systems architecture show how multiple systems link and interoperate, and describe the internal construction and operations of particular systems within the architecture?			
3. For the individual system, does the systems architecture include the physical connection, location, and identification of key nodes (including circuits, networks, etc.)?			
4. Does the system architecture specify system and component performance parameters (e.g., mean time between failure, maintainability, and availability)?			
5. Does the system architecture identify and describe the hardware configuration?			
6. Does the system architecture identify and describe the software configuration?			
7. Does the system architecture identify and describe the firmware to be used in the system?			
8. Does the system architecture identify and describe all system interfaces?			
9. Does the system architecture identify and describe all external connections?			
10. Does the system architecture define the accreditation boundary?			
11. Does the system security architecture implement the security policy and requirements?			
12. Does the architecture state how the security enforcing functions of the system will be provided?			
13. Does the system maintain a domain for its own execution that protects it from external interface or tampering?			
14. Are safeguards in place to detect and minimize inadvertent or malicious modification or destruction of the computer system?			
15. Does the system design documentation accurately reflect a decomposition of the system security policy and requirements into constituent system elements?			

Table AP2.T2. Task 2-2 Level 1 Checklist

Software, Hardware, and Firmware Design Analysis	YES	NO	N/A
1. Was a security analysis conducted to determine the appropriate security requirements?			
2. Was the design specification evaluated and approved for the adequacy of software security measures necessary to meet the security requirements?			
3. Were all the security requirements incorporated in the software?			
4. Does the software security design meet the approval of the DAA?			
5. Does the software design documentation accurately reflect a decomposition of the system security policy and requirements into constituent software elements?			
6. Are security enforcing components identified?			
7. Are non-security-enforcing components identified whose failure or misuse could compromise security?			
8. Is there a close correspondence between the detailed design and the source code and/or hardware drawings?			
9. Were all the general requirements incorporated in the design?			
10. Is there evidence of traceability, such as matrices, tables, or trees, which map the security requirements to software components or modules containing the security designs and implementation?			
11. Does the system design documentation follow the appropriate document standards (DIDs, etc.) with respect to traceability compliance.			
12. Are there complete and appropriate references to other security relevant documents in the design documentation?			
13. Does the operating system support the security requirements?			
14. Does the operating system meet the requirement for identification?			
(a) Are all authorized users uniquely identified before granting access to the system?			
(b) Does the operating system enforce unambiguous USER IDs to identify its users?			
(c) Does the security administrator have a choice of automatic or manual disabling of USER IDs?			
15. Does the operating system meet the requirement for authentication?			
(a) Does the operating system verify the identity of all users prior to allowing access?			
(b) Does the operating system preserve the confidentiality and integrity of stored authentication information such as passwords, PINs, and authentication tokens?			
16. Does the operating system meet the requirement for data and system integrity?			
(a) Does the operating system have the capability to identify the original creator of any named or user-accessible resources such as data and processes?			

Table AP2.T2. Task 2-2 Level 1 Checklist--Continued

Software, Hardware, and Firmware Design Analysis	YES	NO	N/A
17. Does the operating system meet the requirement for audit?			
(a) Does the audit log provide the capability to investigate unauthorized activities after they occur so that proper remedial action can be taken?			
(b) Are the audit requirements defined?			
(c) Does the operating system generate logs that contain information about security relevant events?			
(d) Are items selectable and definable for recording by the security administrator?			
(e) Are audit logs protected from unauthorized access or destruction by means of access controls based on user?			
(f) Are audit logs and audit control mechanisms protected from modification or destruction?			
18. Does the operating system meet the requirement for data confidentiality?			

Table AP2.T3. Task 2-3 Level 1 Checklist

Network Connection Rule Compliance Analysis	YES	NO	N/A
1. Does this system or network connect to any other network or systems?			
2. Are all the network interfaces and communications clearly identified?			
(a) Is there a network configuration diagram available?			
(b) Is there an identification of the information that is allowed to flow across the interface?			
3. Are the security requirements for each side of the interface identified?			
4. Are all security requirements for all interfaces defined?			
5. Do all communications links between remote facilities and the central LAN or central computer facility meet the requirements for the transmission of the highest classification of information to be transferred?			
6. Do all communications links between remote facilities and the central LAN or central computer facility meet the requirements for all categories of data contained in the system?			
7. Are all remote workstations or terminals uniquely identified when accessing the host?			
8. Does the network design comply with the security requirements?			
9. Are MOUs in place for each network interface?			
10. Are procedures in place to ensure that individual nodes of the network comply with the network countermeasures and requirements prior to interfacing with the network?			

Table AP2.T4. Task 2-4 Level 1 Checklist

Integrity Analysis of Integrated Products	YES	NO	N/A
1. Are the COTS and GOTS products certified?			
2. Are the COTS and GOTS products accredited?			
3. Were the products developed by cleared developers or integrators?			
4. Have the COTS or GOTS products been evaluated for security vulnerabilities?			
(a) Have the products been checked for viruses, Y2K compliance, backdoors or trapdoors?			
(b) Is public domain software included in the products?			
(c) Were products developed in the C programming language?			
(d) Is JAVA used in the products?			
(e) Is Active-X used in the products?			
(f) Do the products run in user mode or kernel mode?			
5. Have any modifications been made to previously approved products?			
6. If modifications have been made, have the modifications been evaluated for security vulnerabilities?			

Table AP2.T5. Task 2-5 Level 1 Checklist

Life-Cycle Management Analysis	YES	NO	N/A
1. Is all the software (including the current version number) reflected in the SSAA?			
2. Has all of the software on the system been properly licensed?			
3. Is authenticity of the operating system software verified by comparing the registry or shipment number of the software package with that contained in record communications from the originator?			
4. Is proper documentation available for all software, and are all modules and interfaces described in detail?			
5. Is an inventory of all software maintained?			
6. Are configuration management procedures in place for new additions of new software, updated software and maintenance of software?			
7. Prior to operational use of any new system release does the ISSO conduct sufficient testing to verify that the system meets the security requirements?			
8. Are new releases tested and debugged during dedicated time in a controlled environment?			
9. Are all software patches unique to the site tested by software personnel?			
10. Is the operating system software protected to the highest classification and for all restrictive categories of data which the central system is processing or storing online?			
11. Is there a backup copy of all applications software, operating system and system utilities maintained?			
12. Are the backup copies protected as described in item 10, above.			
13. At a minimum, are all software and backups stored in a fire rated container or off-site location?			
14. Are Configuration Management and Change Controls documented?			
(a) Is the authenticity of the operating system or executive software verified by comparing the registry or shipment number of the software package with that contained in record communications from the originator?			
(b) Prior to operational use of any new system release, does the ISSO conduct sufficient testing to verify that the system meets the documented and approved security specifications?			
(c) Are new releases tested and debugged during dedicated time in a controlled environment?			
(d) Are all software patches tested by system software personnel?			
(e) Does the ISSO or CM Review Board maintain a system baseline and backup?			
(f) Does ISSO maintain and monitor a log of all system patches?			
(g) Has the ISSO developed and approved a method to control access to system tapes or disks?			
(h) Has each individual user been assigned a unique user identification and password that has been randomly machine generated?			

Table AP2.T5. Task 2-5 Level 1 Checklist--Continued

Life-Cycle Management Analysis	YES	NO	N/A
15. Are functional configuration audits performed?			
16. Is there a process in place for requesting and approving system changes before they are made?			
17. Are all system modifications documented and entered into the configuration management baseline?			
18. Are system modifications reflected in the SSAA and are procedures in place to keep the SSAA system configuration current?			

Table AP2.T6. Task 2-6 Level 1 Checklist

Vulnerability Assessment	YES	NO	N/A
1. Have all vulnerabilities identified in tasks 2-1 through 2-5 been documented in the SSAA?			
2. Have the vulnerabilities been analyzed to determine their susceptibility to exploitation?			
3. Have the vulnerabilities been analyzed to determine probability of their occurrence?			
4. Has the threat been properly documented and analyzed to determine the relationship to this system?			
5. Have the threat and vulnerabilities been analyzed to determine the risk to the system operation?			
6. Have additional countermeasures been identified to address the risks?			
7. If any residual risks remain, have they been documented in the SSAA?			
8. Are the residual risks acceptable for operation of this system?			
9. Have ST&E procedures been developed to evaluate the high risk areas?			
10. Is this system ready for full-scale integration and to progress to Phase 3?			

Table AP2.T7. Task 3-1 Level 1 Checklist

Security Test and Evaluation (ST&E)	YES	NO	N/A
1. Has a system ST&E plan been prepared and is it sufficient to ensure thorough examination and exercising of the system's security confidentiality, integrity and availability control features and procedures to determine their effectiveness and reliability?			
2. Have system ST&E procedures been prepared?			
(a) Are the procedures sufficiently comprehensive to ensure thorough examination and exercising of the system's security confidentiality control features and procedures to determine their effectiveness and reliability?			
(b) Are the procedures sufficiently comprehensive to ensure thorough examination and exercising of the system's security integrity control features and procedures to determine their effectiveness and reliability?			
(c) Are the procedures sufficiently comprehensive to ensure thorough examination and exercising of the system's security availability control features and procedures to determine their effectiveness and reliability?			
(d) Are the procedures sufficiently comprehensive to ensure thorough examination and exercising of the system's security accountability control features and procedures to determine their effectiveness and reliability?			
(e) Are the procedures traceable to the security requirements in the RTM?			
(f) Are all security requirements tested?			
3. Have tools been identified to support the ST&E?			
(a) Have the tools been procured with sufficient licenses to test the entire system or network?			
(b) Will the ISSO or system manager retain a copy of the tool and a license to run the tool?			
(c) Are any proprietary tools being used? If so, how will the Government obtain use of the tool for periodic retesting?			
4. Has the ST&E been performed?			
5. Have the results of the ST&E been documented in the SSAA?			
6. Have the ST&E results been analyzed to identify any vulnerabilities of this system?			
7. Have the vulnerabilities been documented in the SSAA?			
8. Does the ISSO maintain a copy of the ST&E plan and results?			

Table AP2.T8. Task 3-2 Level 1 Checklist

Penetration Testing	YES	NO	N/A
1. Is there an announced/unannounced monitoring/penetration vulnerability assessment process or procedures in place?			
2. Are vulnerabilities and discrepancies analyzed to determine their susceptibility to exploitation?			
3. Does the system have any intrusion detection or real time monitoring software installed?			
4. Are network analysis tools used to monitor the integrity of the system?			

Table AP2.T9. Task 3-3 Level 1 Checklist

TEMPEST and RED/BLACK Verification	YES	NO	N/A
1. If TEMPEST requirements apply to this system, has a Red-Black inspection been conducted?			
2. Are the results of the Red-Black inspection acceptable?			
3. If TEMPEST requirements apply to this system, has TEMPEST testing been conducted?			
4. If TEMPEST testing has been conducted, are the results acceptable or is the physical control zone sufficient?			
5. Has NTISSI 7000 been used to determine the applicable TEMPEST countermeasures for computer systems processing classified material?			
6. Were the countermeasures implemented and maintained?			

Table AP2.T10. Task 3-4 Level 1 Checklist

COMSEC Compliance Validation	YES	NO	N/A
1. Have COMSEC protective measures been implemented to protect the transmission of classified and/or sensitive information?			
2. If classified information is being transmitted is it being protected by NSA-approved Type 1 encryption equipment and keying material?			
3. If sensitive information is being transmitted, is it being protected by products which conform to DES in FIPS PUB 46-1 and FIPS PUB 140 or their successors?			
4. If sensitive information being transmitted is not protected by DES products, has a waiver to these standards been granted pursuant to Section 3506(b) of Title 44 U.S. Code?			
5. If sensitive information is being transmitted is it being protected by NSA-approved Type 1 encryption equipment and keying material?			
6. If classified or sensitive information is being transmitted is it protected by a PDS?			

Table AP2.T11. Task 3-5 Level 1 Checklist

System Management Analysis	YES	NO	N/A
1. Has a Computer System Security Program been established?			
2. Has the system (and all applications and network) been accredited?			
(a) Did the accreditation use the DITSCAP process?			
(b) Has a SSAA been developed?			
(c) Has the SSAA been approved?			
3. Has the DAA determined if a risk assessment is required?.			
(a) Has a risk assessment been performed?			
(b) Does the ISSO maintain a copy of the risk assessment?			
(c) Is the risk assessment kept updated and repeated?			
(d) Is the risk assessment updated when any change is made to the facility, IT equipment, system software, or application software that affects the overall IT security posture?			
(e) Is the risk assessment updated when any change is made in operational configuration, data sensitivity, or classification level?			
(f) Is the risk assessment updated when any change is made that appears to invalidate the original conditions of accreditation?			
4. Is the system reaccredited when any change is made to the facility, IT equipment, system software, or application software that affects the overall IT security posture?			
5. Is the system reaccredited when any change is made in operational configuration, data sensitivity, or classification level?			
6. Is the system reaccredited when any change is made that appears to invalidate the original conditions of accreditation?			
7. Has an ISSO been appointed in writing?			
8. Is the ISSO the focal point for all security matters for the IT systems assigned?			
9. Have the duties and responsibilities of the ISSO been defined in writing?			

Table AP2.T11. Task 3-5 Level 1 Checklist--Continued

System Management Analysis	YES	NO	N/A
10. Do the ISSO duties include the following:			
(a) Executing the Computer Security Program as it applies to the assigned IS including preparing and supporting the accreditation support documentation.			
(b) Maintaining an inventory of IS hardware, system software, and major functional application systems?			
(c) Monitoring system activity, e.g., identification of the levels and types of data handled by this IS system, assignment of passwords, review of audit trails, etc., to ensure compliance with security directives and procedures?			
(d) Security oversight and monitoring of remote IS components or to ensure compliance with security requirements?			
(e) Conducting and documenting risk assessments for the assigned IS?			
(f) Supervising, testing and monitoring changes in the IT system affecting the IT activity posture as appropriate?			
(g) Implementing or overseeing the implementation of appropriate countermeasures?			
(h) Implementing or overseeing the implementation of the Security and Training and Awareness Program?			
(i) Monitoring IT procurement for security impact to ensure compliance with security regulations and known security requirements for the assigned IS?			
(j) Ensuring that all IT security incidents or violations are investigated, documented and reported to appropriate authorities?			
11. Has the ISSO developed and approved a method to control access to system tapes or disks?			
12. Does the ISSO maintain a copy of the ST&E plan and results?			
13. Has each individual user been assigned a unique user identification and password that has been randomly machine generated?			

Table AP2.T12. Task 3-6 Level 1 Checklist

Site Accreditation Survey	YES	NO	N/A
1. Has a Site Survey been completed?			
2. Has the system been Certified and Accredited previously?			
3. Does the computer facility meet the following requirements:			
(a) Is the system operated within the manufacturer's optimum temperature and humidity range specifications?			
(b) Are environmental systems dedicated to the computer facility?			
(c) Are environmental controls regulated by key designated personnel only?			
(d) Is a temperature/humidity recording instrument installed to monitor the system area?			
(1) Is the temperature/humidity instrument connected to an alarm to warn of near-limit conditions?			
(e) Is adequate lighting present?			
(f) Is emergency lighting available ?			
(g) Is electrical power reliable?			
(h) Are voltage regulators or other electronic devices present to prevent serious power fluctuations?			
(i) Does the facility have an interruptible power source?			
(j) Are cleaning procedures and schedules established and adhered to?			
(k) Is the facility overhead free of steam and water pipes?			
(l) Are plastic sheets available to protest the system from water damage?			
(m) Is there a facility fire bill?			
(n) Are emergency exits clearly marked?			
(o) Do employees receive periodic training in the following areas:			
(1) Power shut down and start up procedures?			
(2) Operation of emergency power?			
(3) Operation of fire detection and alarm systems?			
(4) Operation of fire suppression equipment?			
(5) Building evacuation procedures?			
(p) Is a master power switch or emergency cut-off switch to IT equipment present?			
(q) Is the master power switch located near the main entrance of the IT area?			
(r) Is the master power switch adequately labeled, or protected by a cover, to prevent accidental shut off?			
(s) If the system process critical applications, has a sequential shutdown routine?			
(t) Do a sufficient number of portable fire extinguishers exist?			
(u) Does a central fire suppression system exist?			
(v) Is automatic smoke/fire detection equipment present?			
(w) Does the fire/smoke system activate an alarm at the nearest fire station?			

Table AP2.T13. Task 3-7 Level 1 Checklist

Contingency Plan Evaluation	YES	NO	N/A
1. Is there a contingency plan in existence for this system?			
2. Does the contingence plan, at a minimum, address the following:			
(a) The actions required to minimize the impact of a fire, flood, civil disorder, natural disaster, or bomb threat?			
(b) Backup procedures to conduct essential IS operational tasks after a disruption to the primary IS facility?			
(c) Recovery procedures to permit rapid restoration of the IS facility following physical destruction, major damage or loss of data?			
3. Does this contingency plan provide for the following:			
(a) Storage of system back-up data in off site storage or in the central computer facility in metal or other fire retardant cabinets?			
(b) Duplicate system tapes, startup tapes/decks, database save tapes, and application program tapes unique to the site to be maintained in a secure location removed from the central computer facility?			
(c) Identification of an alternate site containing compatible equipment?			
(d) Destruction or safeguarding of classified material in the central computer facility in the event that the facility must be evacuated?			
4. Has the contingency plan been tested during the past year?			
5. Does the ISSO maintain a copy of the contingency plan?			
6. Does the contingency plan contain criteria to state when it should be implemented and whom can make that decision?			

Table AP2.T14. Task 3-8 Level 1 Checklist

Risk Management Review	YES	NO	N/A
1. Has the DAA determined if a risk assessment is required?			
2. Has a risk assessment been performed?			
(a) Are risk analysis and incident response procedures documented?			
(b) Does the ISSO maintain a copy of the risk assessment?			
(c) Is the risk assessment kept updated and repeated?			
3. Have all vulnerabilities identified in tasks 2-1 through 2-5 been documented in the SSAA?			
4. Have the vulnerabilities been analyzed to determine their susceptibility to exploitation?			
5. Have the vulnerabilities been analyzed to determine probability of their occurrence?			
6. Has the threat been properly documented and analyzed to determine the relationship to this system?			
7. Have the threat and vulnerabilities been analyzed to determine the risk to the system operation?			
8. Have additional countermeasures been identified to address the risks?			
9. If any residual risks remain, have they been documented in the SSAA?			
10. Are the residual risks acceptable for operation of this system?			
11. Have ST&E procedures been developed to evaluate the high-risk areas?			
12. Is this system ready for accreditation and to progress to Phase 4?			