NSTISSI No. 1000
April 2000

National Information Assurance Certification and Accreditation Process (NIACAP)

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER INFORMATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

FOREWORD

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), establishes the minimum national standards for certifying and accrediting national security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site. This process focuses on an enterprise-wide view of the information system (IS) in relation to the organization's mission and the IS business case.

2. The NIACAP is designed to certify that the IS meets documented accreditation requirements and will continue to maintain the accredited security posture throughout the system life cycle.

3. Representatives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) may obtain additional copies of this instruction at the address listed below.

MICHAEL V. HAYDEN
Lieutenant General, USAF
National Manager

NSTISSC Secretariat (I42). National Security Agency.9800 Savage Road STE 6716. Ft Meade MD 20755-6716
(410) 854-6805.UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

National Information Assurance Certification and Accreditation Process (NIACAP)

NIACAP Purpose ..... Section 1
NIACAP Scope ..... Section 2
NIACAP Roles ..... Section 3
SSAA Description ..... Section 4
NIACAP Phases ..... Section 5
Phase 1, Definition ..... Section 6
Phase 2, Verification ..... Section 7
Phase 3, Validation ..... Section 8
Phase 4, Post Accreditation ..... Section 9
NIACAP Roles and Federal Agency Management Organization ..... Section 10
Department and Agency Level Management ..... Section 11
NIACAP Roles and Responsibilities ..... Section 12

SECTION 1 – NIACAP PURPOSE

1. This National Security Telecommunications and Information System Security Instruction (NSTISSI) defines the National Information Assurance Certification and Accreditation Process (NIACAP). The NIACAP establishes a standard national process, set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site. This document provides an overview of the NIACAP process, roles of the people involved, and the documentation produced during the process. More detailed procedures will be included in a NIACAP implementation manual.

2. The process is designed to certify that the information system (IS) meets documented security requirements and will continue to maintain the accredited security posture throughout the system life cycle. The process should be adapted to include existing system certifications and evaluations of products. Users of the process must align the process with their program strategies and integrate the activities into their enterprise system life cycle. While the NIACAP maps to any system life cycle process, its four phases are independent of the life cycle strategy. While developed for national security systems, the NIACAP may, at an agency's discretion, be adapted to any type of IS and any computing environment and mission subject to the policies found in OMB Circular A-130, Appendix III and the standards and guidance issued by the National Institute of Standards and Technology (NIST).

3. The key to the NIACAP is the agreement between the IS program manager[1], Designated Approving Authority (DAA)[2], certification agent (certifier), and user representative. These individuals resolve critical schedule, budget, security, functionality, and performance issues.

4. The NIACAP agreements are documented in the System Security Authorization Agreement (SSAA). The SSAA is used to guide and document the results of the Certification and Accreditation (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

[1]Program manager will be used in this document to refer to the program manager responsible for system acquisition or development, the system manager during operation of the system, or the maintenance organization's program manager when a system is undergoing a major change.

[2]The DAA is also referred to as the accreditor in this document. The term DAA will be used as singular term; however, in many cases the actions by the DAA may be joint actions by multiple DAAs or a single DAA representing multiple DAAs for type accreditation situations.

a system are made. After accreditation, the SSAA becomes the baseline security configuration document.

SECTION 2 - NIACAP SCOPE

5. The National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 6 establishes the requirement for federal departments and agencies to implement a C&A process for national security systems under their operational control. This NSTISSI provides guidance on how to implement the NSTISSP No. 6 policy. The requirements of the NSTISSI apply to all U.S. Government Executive Branch departments, agencies, and their contractors and consultants. This document is issued and maintained by the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

SECTION 3 - NIACAP ROLES

6. The minimum NIACAP roles include the program manager, DAA, certifier, and user representative. Additional roles may be added to increase the integrity and objectivity of C&A decisions. For example, the Information Systems Security Officer (ISSO) usually performs a key role in the maintenance of the security posture after the accreditation and may also play a key role in the C&A of the system.

7. The program manager represents the interests of the system throughout its life cycle management (acquisition, life cycle schedules, funding responsibility, system operation, system performance, and maintenance). The DAA is an executive 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 determines the acceptable level of residual risk for a system. The certifier provides the technical expertise to conduct the certification throughout the system's life cycle based on the security requirements documented in the SSAA. The certifier should be independent from the organization responsible for system development. The operational interests of system users are vested in the user representative. Detailed roles and responsibilities will be defined in Sections 10-12.

SECTION 4 - SSAA DESCRIPTION

8. The SSAA documents the conditions of the C&A for an IS. The SSAA is a formal agreement among the DAA(s), certifier, user representative, and program manager. The SSAA is used throughout the entire NIACAP 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 SSAA has the following characteristics:

- Describes the operating environment and threat.
- Describes the system security architecture.
- Establishes the C&A boundary of the system to be accredited.
- Documents the formal agreement among the DAA(s), certifier, program manager, and user representative.
- Documents all requirements necessary for accreditation.
- Minimizes documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations, architecture description, test procedures, etc).
- Documents the NIACAP plan.
- Documents test plans and procedures, certification results, and residual risk.
- Forms the baseline security configuration document.

9. There are different types of accreditation depending on what is being certified. A system accreditation evaluates a major application or general support system. A site accreditation evaluates the applications and systems at a specific, self-contained location. A type accreditation evaluates an application or system that is distributed to a number of different locations. The NIACAP applies to each of these accreditation types and may be tailored to meet the specific needs of the organization and IS.

10. Each information system must be covered by an SSAA. In some cases a single SSAA may include several systems. For type accreditations, 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 will receive confirmation and documentation of the type of certification and accreditation. 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.

11. The physical characteristics of the SSAA will depend on the certification complexity and organizational requirements. The SSAA can be as simple as 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 can be tailored to incorporate other documents as appendices or by reference.

12. The DAA, certifier, program manager, and user representative have the authority to tailor the SSAA to meet the characteristics of the IS, operational requirements, security policy, and prudent risk management. The SSAA must be 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 may change. When that occurs, the SSAA is updated to accommodate the new components. The SSAA is developed in Phase 1 and 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, program manager, and user representative. The support organizations must understand each of these essential items.

13. If multiple DAAs are involved, a single DAA may be identified to represent them. The agreement between the DAAs should be included with the SSAA.

14. 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 IA certification, test beds, test development, testing, and accreditation. The SSAA is a binding agreement between all government and government contractor entities involved in the IS. The provisions for developing and implementing the SSAAs must be included in contractual documents between the government and its contractors.

SECTION 5 - NIACAP PHASES

15. The NIACAP is composed of four phases (Figure 1): Definition, Verification, Validation, and Post Accreditation. Phase 1, Definition, is focused on understanding the IS business case, environment, and architecture to determine the security requirements and level of effort necessary to achieve certification and accreditation. The objective of Phase 1 is to agree on the security requirements, C&A boundary, schedule, level of effort, and resources required.

Phase 2, Verification, verifies the evolving or modified system's compliance with the information in the SSAA. The objective of Phase 2 is to ensure the fully integrated system will be ready for certification testing.

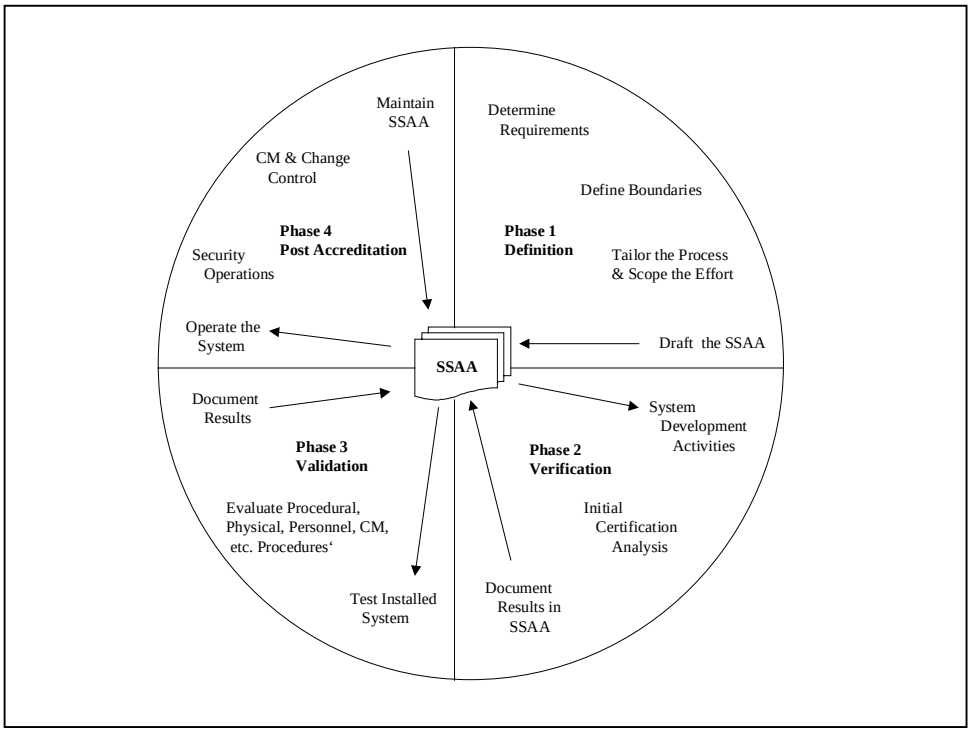


Figure 1. A Notional View of the NIACAP

16. Phase 3, Validation, validates compliance of the fully integrated system with the security policy and requirements stated in the SSAA. The objective of Phase 3 is to produce the required evidence to support the DAA in making an informed decision to grant approval to operate the system (accreditation or Interim Approval to Operate (IATO)). Phase 4, Post Accreditation, starts after the system has been certified and accredited for operations. Phase 4 includes those activities necessary for the continuing operation of the accredited IS in its computing environment and to address the changing threats and small scale changes a system faces through its life cycle. The objective of Phase 4 is to ensure secure system management, operation, and maintenance to preserve an acceptable level of residual risk.

17. The NIACAP phases are comprised of activities. The activities include tasks and procedures. Each phase and activity should be performed. The tasks in each activity may be tailored and scaled to the system and its associated acceptable level of residual risk. The implementation is expected to be tailored and integrated with on-going systems acquisition activities to best fit the mission, environment, system architecture, and programmatic considerations. The process is flexible, but must be tailored to deal with different organizations, acquisition strategies, and operational scenarios.

18. The following sections describe the phases, activities, and tasks required. Additional details on the process will be provided in a NIACAP implementation manual. The implementation manual will be prepared by the NSTISSC at a later date.

SECTION 6 - PHASE 1, DEFINITION

19. Phase 1 tasks define the C&A level of effort, identify the principle C&A roles and responsibilities, and culminates with an agreement on the method for implementing the security requirements. This agreement is documented in the SSAA.

20. Phase 1 (Figure 2) contains three activities – preparation, registration, and negotiation. Phase 1 starts with a review of the system and site related documents and ends by producing the SSAA. The NIACAP process is started when the concept design of a new information system or modification to an existing system is begun in response to an identified business case, operational requirement, or mission need. Any security relevant changes should initiate the NIACAP for any existing or legacy IS. When recertifying legacy systems, the available C&A documentation should be converted to the NIACAP SSAA format.

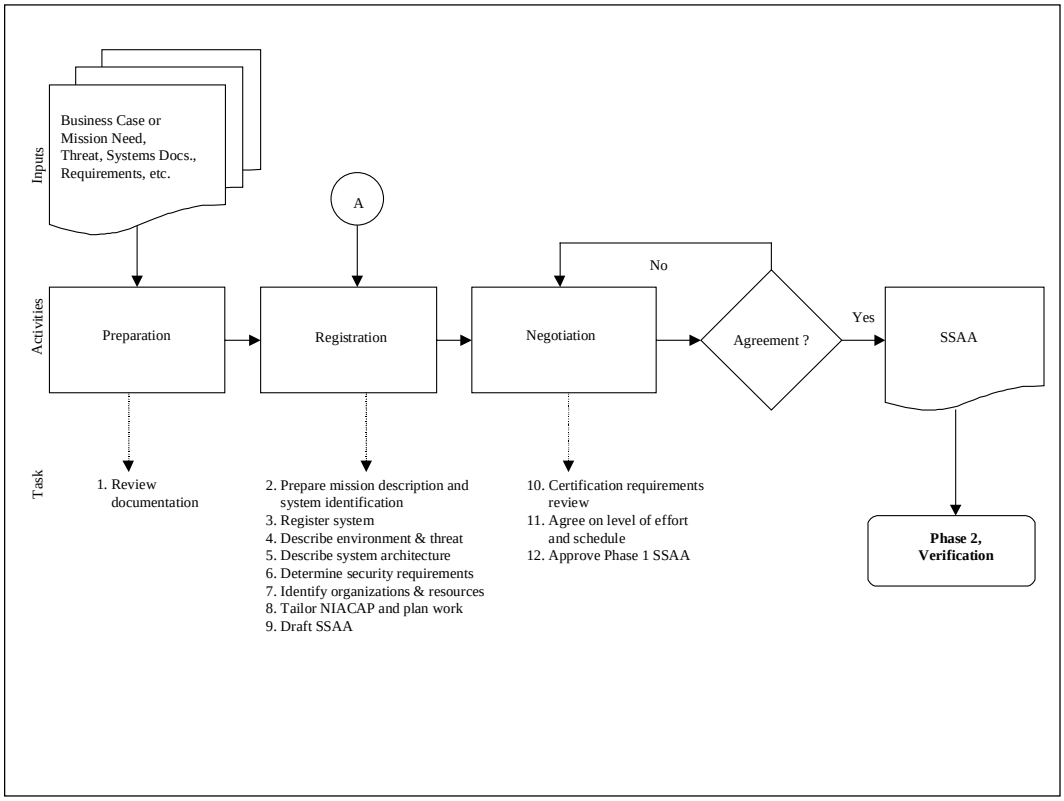


Figure 2. NIACAP Phase 1, Definition

21. Preparation - 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 Need Statement, system specifications, architecture and design documentation, users manuals, operating procedures, network diagrams, and configuration management documentation, if available. National, agency, and organizational level security instructions and policies should be collected and reviewed. The following list identifies the types of information collected and reviewed during the preparation phase:

- Business Case
- Mission Need Statement
- System Specifications
- Architecture and Design Documents
- User Manuals
- Operating Procedures
- Network Diagrams
- Configuration Management Documents
- Threat Analysis
- Federal and Organization IA and Security Instructions and Policies

22. Registration - Registration initiates the risk management agreement process among the DAA, certifier, program manager, and user representative. Information is evaluated, applicable IA requirements[3] 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 mission description and system identification and concludes with preparing an initial draft of the SSAA.

a. 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 include the following:

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

b. 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 facility equipment that is to be addressed in the C&A. Therefore, the IS facilities and equipment must be under the control of the DAA. Any facility or equipment that is not to be considered or is not under the control of the DAA should be considered as external interfaces. Additionally, known threats should be assessed against the specific system functions and system descriptions 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.

c. The NIACAP 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's business functions, national,

[3]IA requirements may be defined by each department or agency, or may be developed from International Standard 15408, the Common Criteria.

departmental, and agency security requirements, criticality of the system to the organizational 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 NIACAP certification tasks must be performed at one of these four levels of certification.

d. The SSAA is prepared during the registration activities[4]. When registration activities are concluded, the draft SSAA is submitted to the DAA, certifier, program manager, and user representative. The draft SSAA is then used as the basis for discussions during the negotiation phase.

23. Negotiation - Negotiation is the NIACAP activity where all the participants[5] involved in the IS's development, acquisition, operation, security certification, and accreditation agree on the implementation strategy to be used to satisfy the security requirements identified during system registration. The negotiation tasks are listed below.

- Conduct the certification requirement review (CRR).
- Agree on the security requirements, level of effort, and schedule.
- Approve final Phase 1 SSAA.

a. Negotiation starts with a review of the draft SSAA. The DAA conducts a complete review of the draft SSAA to determine that all appropriate IA and security requirements are included. The certifier conducts a comprehensive evaluation of the technical and nontechnical security features of the IS. 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 efforts and resource requirements to determine that the appropriate assurance is being applied.

b. A CRR must be held for the C&A participants. The CRR 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).

c. The purpose of negotiation is to ensure that the SSAA properly and clearly defines the approach and level of effort. During the negotiations, all participants will 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.

---

[4]The SSAA is normally drafted by the program manager, but may be drafted by the certifier (certification team).

[5]These individuals may choose to designate someone to represent them in the negotiations. Unless noted, the terms will be used interchangeably to mean the principle or their designated representative, and the staff that supports them.

SECTION 7 - PHASE 2, VERIFICATION

24. The Phase 2 activities (Figure 3) 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 formal C&A of the system. Phase 2 activities verify security requirements during system development or modification by certification analysis and assessment of the certification results. The SSAA is refined during Phase 2.

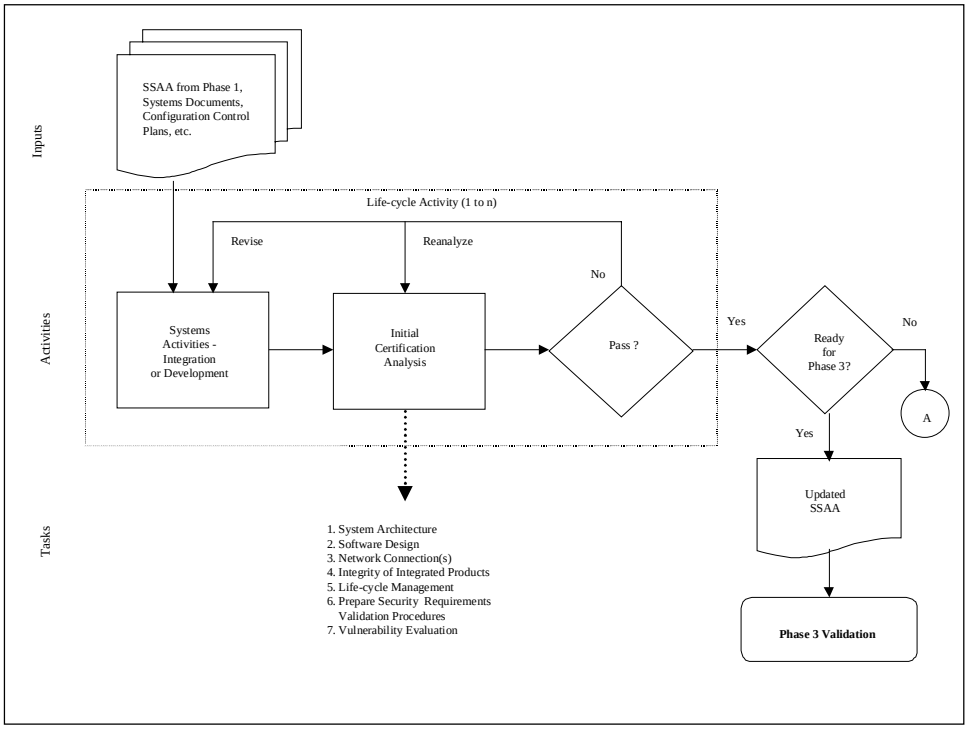


Figure 3. NIACAP Phase 2, Verification

25. Refine the SSAA - Phase 2 starts with a review of the SSAA. The SSAA is updated throughout Phase 2 to include changes made during system development or modifications and to include the results of the certification analysis. At each stage of 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.

26. System Development and Integration - System development and integration activities are those activities required for development or integration of the information system 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 information system in the life cycle. During system development and integration, there are corresponding Phase 2 certification analysis tasks. The certification analysis tasks verify that the requirements in the SSAA are met in the evolving system before it is integrated into the operating environment. System development and integration tasks could include the following:

- Prepare system architecture.
- Prepare high level and detailed design documents.

- Integrate Commercial-off-the-Shelf (COTS) products.
- Conduct system integration testing.

27. Initial Certification Analysis - The initial certification analysis determines if the IS is ready to be evaluated and tested under Phase 3, Validation activities. Certification verifies that the development, modification, and integration efforts will result in a higher probability of success for an accreditable IS before Phase 3 begins.

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

- System architecture analysis
- Software, hardware, and firmware design analysis
- Network connection rule compliance analysis
- Integrity analysis of integrated products
- Life cycle management analysis
- Security requirements validation procedure preparation
- Vulnerability assessment

b. When the Phase 2 initial certification analysis is completed, the system should have a documented security specification, comprehensive test procedures, and written assurance that all network and other interconnection requirements have been implemented. When systems are being deployed to multiple locations, their planned interfaces with other components of the operating environment must be verified. COTS and government off-the-shelf (GOTS) products used in the system must be verified to assure that they have been integrated properly and that their functionality meets the security and operational requirements of the system. Life cycle management plans will be analyzed to verify that sufficient plans and procedures are in place to maintain the security posture. Phase 3 test procedures will be prepared as applicable. Phase 2 tasks conclude with a vulnerability assessment to identify the residual risk.

(1) System Architecture Analysis - This certification task verifies that the system architecture complies with the architecture description in the SSAA. 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. Those interfaces must be evaluated to assess their effectiveness in maintaining the security posture of the infrastructure.

(2) Software, Hardware and Firmware Design Analysis - The software, hardware and firmware design analysis task evaluates how well the software, hardware and firmware reflect the security requirements of the SSAA and the security architecture of the system. This task may, for example, include a detailed analysis of software specifications and software design documentation. The design analysis task must assess whether critical security features (identification and authentication, access controls, auditing, etc.) are implemented correctly and completely.

(3) Network Connection Rule Compliance Analysis - 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. Test plans and procedures must be developed to validate compliance with the network connection rules.

(4) Integrity Analysis of Integrated Products - This task evaluates the integration of COTS, GOTS, or Non-Developmental Item(s) (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. Integrity analysis of products being integrated into the system must identify the security functionality of each product. The product security functionality should be verified by the certification team 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 the system and subsystem interfaces, examination of product evaluations by NIST or the National Computer Security Center (NCSC), information flows, and applicable use of selectable product features.

(5) Life Cycle Management Analysis - The life cycle management analysis task verifies that change control and configuration management 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 following types of documents or procedures:

- Life cycle management plan
- Configuration identification procedures
- Configuration control procedures
- Configuration status accounting procedures
- Configuration audit procedures and reports
- Software engineering (development approach and engineering environment) procedures
- System distribution plans

(6) Security Requirements Validation Procedure Preparation - In this task, the certification team defines the procedures to be used to verify compliance with all the defined security requirements. The security requirements document must identify the type of review required to validate each requirement. If test procedures are prepared, they should be added to the SSAA. At certification Level 1, the test procedures may be a detailed checklist (will be available in the NIACAP Implementation Manual). At certification Levels 2 through 4, a test, observation, document review, or interview procedure should verify each requirement.

(7) Vulnerability Assessment - This task evaluates security vulnerabilities with regard to confidentiality, integrity, availability, and accountability and recommends applicable countermeasures. The DAA should determine the acceptable level of risk to protect the system commensurate with its value to the federal agency.[6] In Phase 2, the vulnerability assessment concentrates on verifying the implementation of the security requirements.

[6]An acceptable level of residual risk is based on the relationship of the threat to the system and the information processed; to the information system's mission, environment, and architecture; and its security confidentiality, integrity, availability, and accountability objectives.

(a) During vulnerability assessment, each of the vulnerabilities and discrepancies isolated during the evaluation of the system architecture, system design, network interfaces, product integration, and configuration management practices is analyzed to determine its susceptibility to exploitation, the potential rewards to the exploiter, the probability of occurrence, and any related threat. The analysis should use techniques such as static penetration, flaw hypothesis, and threat-vulnerability pairing to determine the ability to exploit the vulnerabilities. The residual risk, that portion of risk that remains after security measures have been applied, should be determined by ranking the evaluated vulnerabilities against threat, ease of exploitation, potential rewards to the exploiter, and a composite of the three areas. All residual risks must be identified and evaluated. The evaluation should indicate the rationale as to why the risk should be accepted or rejected, and the operational impacts associated with these risks. The results of the Phase 2 vulnerability analysis should be used to guide and scope all Phase 3 test activities.

(b) Coordination among the DAA, certifier, program manager, and user representative ensures that the residual risk does not exceed the level of risk established by the DAA. That level of risk, the "acceptable level of residual risk," must be documented in the SSAA. If the risk exceeds the maximum acceptable risk, the system must return to Phase 1 for reconsideration of the IS business functions, operating environment, and IS architecture.

(8) Assess Analysis Results - At the conclusion of each development or integration milestone, the certification analysis results are reviewed for SSAA compliance. If the results indicate significant deviation from the SSAA, the NIACAP should return to Phase 1 to resolve the problems. If the results are acceptable, the NIACAP proceeds to the next task or to` NIACAP Phase 3.

SECTION 8 - PHASE 3, VALIDATION

28. Phase 3 activities (Figure 4) 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 culminate in the accreditation of the IS (for systems in development, this phase occurs after system integration). Phase 3 includes a review of the SSAA, an evaluation of the integrated IS, certification, and accreditation.

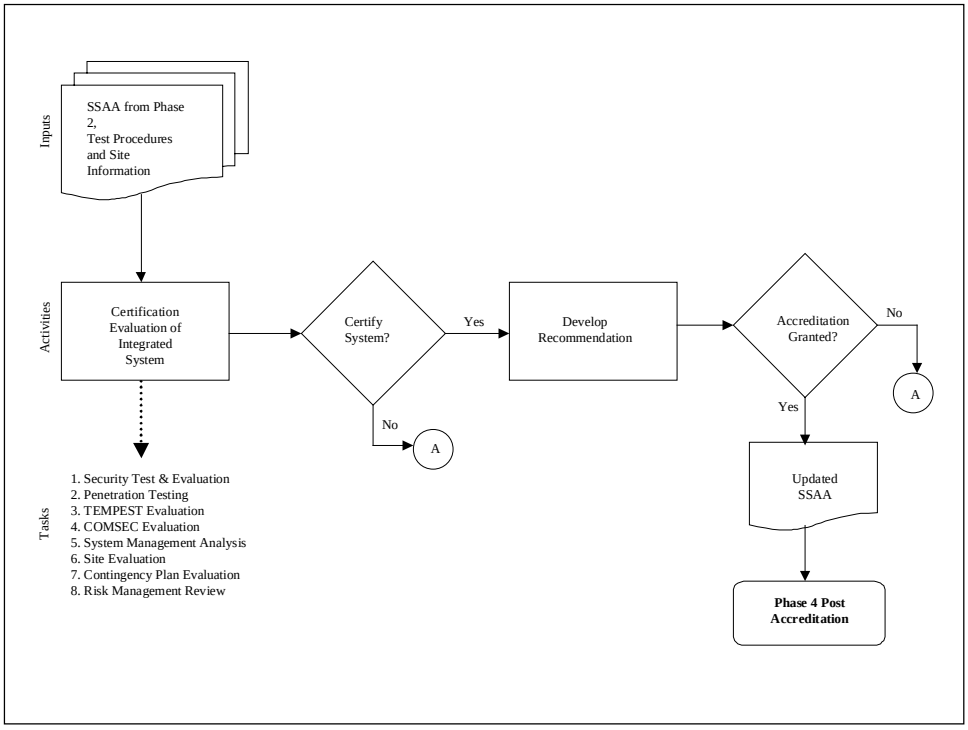


Figure 4. NIACAP Phase 3, Validation

29. Refine the SSAA - 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 document reflecting the current state of the system and refining the SSAA. Required changes must be submitted to the DAA, certifier, program manager, and user representative so that the revised agreement may be approved and implemented.

30. Certification Evaluation of the Integrated System - This activity certifies that the fully integrated and operational system complies with the requirements stated in the SSAA and the system operates with an acceptable level of residual risk. During this activity, certification tasks are performed to ensure that the IS is functionally ready for operational deployment. The certification tasks and the extent of the tasks will depend on the level of certification analysis in the SSAA. The certification tasks may include:

- Security Test and Evaluation (ST&E)
- Penetration Testing
- TEMPEST and RED-BLACK Verification
- Validation of Communication Security (COMSEC) Compliance
- System Management Analysis
- Site Evaluation
- Contingency Plan Evaluation
- Risk Management Review

Phase 3 certification tasks must include certification of the software, firmware, and hardware and inspections of operational sites to ensure their compliance with the physical security, procedural security, TEMPEST, and COMSEC requirements. Phase 3 includes tasks to certify the compatibility of the computing environment with the description provided in the SSAA. NIACAP 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. The paragraphs below describe the certification tasks that may be included in the evaluation of the integrated system.

(1) Security Test and Evaluation - The objective of the ST&E is to assess 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. ST&E validates the correct implementation of identification and authentication, audit capabilities, access controls, object reuse, trusted recovery, and network connection rule compliance.

(a) Individual tests evaluate system conformance with the requirements, mission, environment, and architecture as defined in the SSAA. Test plans and procedures should address all the security requirements and provide sufficient evidence of the amount of residual risk. The test results must validate the proper integration and operation of all security features.

(b) When a system is developed for deployment to multiple locations a type accreditation may be feasible. In this situation, the ST&E should occur at a central integration and test facility or one of the intended operating sites if such a facility is not available. Software and hardware security tests of common system components at multiple sites are not recommended. However, the system installation and security configuration should be tested at each operational site at the time of installation. At the conclusion of the type accreditation ST&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 tests conducted by the type accreditation effort.

(2) Penetration Testing - 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.

(3) TEMPEST and RED-BLACK Verification - TEMPEST and RED-BLACK verification may be required to validate that the equipment and site meet the security requirements. In these situations, the equipment should be TEMPEST tested prior to government acceptance. After installation the site should be inspected to determine if the environment is adequate and that adequate practices are being followed.

(4) Validation of COMSEC Compliance - This task validates that NSA-approved COMSEC is in use and that approved COMSEC key management procedures are used. COMSEC analysis evaluates how well the COMSEC materials and procedures meet the requirements defined in the SSAA.

(5) System Management Analysis - 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 the security policies, system and security management organizations, security training and awareness, rules of behavior, incident response plan and procedures, virus detection procedures, and the configuration management organization and processes. These components may provide insight into security of operations at the site.

(a) The roles and responsibilities assigned to the ISSO must be examined 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 manage the IS security configuration controls, report security incidents, and implement security changes.

(b) Knowledge of the security management structure may provide insight into the emphasis the organization places on secure operation of the computing environment. It also provides an indication of the effectiveness of the security personnel. The effectiveness of the security training and awareness must be examined to provide insight into potential security problem areas.

(c) An effective configuration management program is mandatory if an established security posture is to be maintained. The system management analysis task evaluates the change control and configuration management practices to determine their ability to preserve the integrity of the security relevant software and hardware. A system baseline that identifies all hardware, software, and firmware components and external interfaces, supports 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.

(6) Site Evaluation - The site evaluation task validates that the site operation of the information system is accomplished as documented in the SSAA. The site evaluation 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 system in ships or aircraft) the IS must be examined in representative sites or environments.

(7) Contingency Plan Evaluation - The contingency plan evaluation task analyzes the contingency, back-up, and continuity of service plans to ensure the plans are consistent with the requirements identified in the SSAA. The plans should consider natural disasters, enemy actions, or malicious actions. Periodic testing of the contingency plan is required by Office of Management and Budget, OMB A-130 (Ref. 2) for critical systems and is encouraged for all systems.

(8) Risk Management Review - 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. This is the final review before developing the recommendation to the DAA.

31. Develop Recommendation to the DAA - This activity begins after completion of all certification tasks and ends with a system accreditation recommendation. The purpose of this activity is to consolidate the findings developed during certification of the integrated system and submit the certifier's report to the DAA.

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

b. 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 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.

c. 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.

32. 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 information necessary to support the certifier's recommended decision including security findings, deficiencies, risks to operation, and actions to resolve any deficiencies.

a. If the decision is to accredit, the decision must include the security parameters under which the information system 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.

b. If the decision is made to not authorize the system to operate, the NIACAP process reverts to Phase 1 and the DAA, certifier, program manager, and user representative must agree to the proposed solutions to meet an acceptable level of risk. The decision must state the specific reasons for denial and, if possible, provide suggested solutions.

c. When the system accreditation has been issued, the acquisition or development organization normally will move the responsibility for the SSAA to the system operator or the maintenance organization for the IS. When a decision is made to accredit the system, the NIACAP begins Phase 4.

d. In some situations a common set of software, hardware, or 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 be operated. 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.

SECTION 9 - PHASE 4, POST ACCREDITATION

33. Phase 4 contains activities required to continue to operate and manage the system so that it will maintain an acceptable level of residual risk (Figure 5). Post-accreditation activities

must include ongoing maintenance of the SSAA, system operations, security operations, change management, and compliance validation.

34. Phase 4 begins after the system has been accredited. Phase 4 must continue until the information system is removed from service, a major change is planned for the system, or a periodic compliance validation is required. In the first case, the NIACAP responsibilities of the acquisition organization shift to the system manager or designated maintenance organization. In the other two cases, the NIACAP reverts to Phase 1.

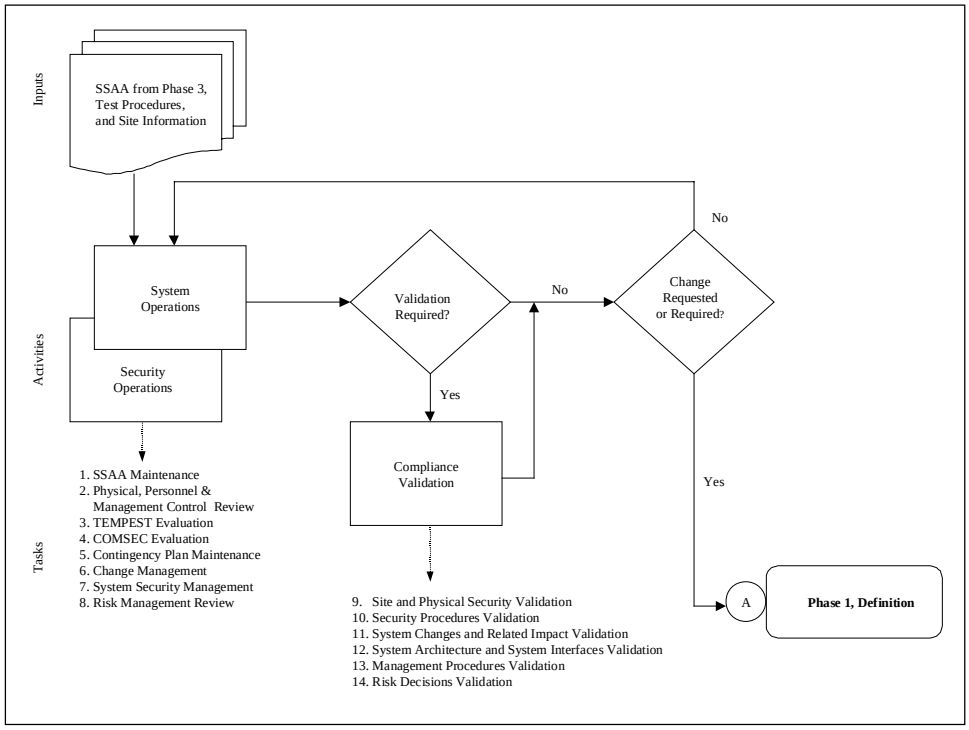


Figure 5. NIACAP Phase 4, Post Accreditation

35. System and Security Operations - The system operation activity concerns the secure operation 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.

a. Secure system management 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 information system 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 information system 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.

b. Secure system management 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 information

system and its computing environment. Secure system management is a continuous review and approval process that involves the users, ISSOs, acquisition or maintenance organizations, configuration management officials, and DAA. The Phase 4 security tasks are described below:

- SSAA Maintenance
- Physical, Personnel, and Management Control Review
- TEMPEST Evaluation
- COMSEC Evaluation
- Contingency Plan Maintenance
- Change Management
- System Security Management
- Risk Management Review

(1) SSAA Maintenance - Phase 4 involves ongoing review of the SSAA to ensure it remains current. The user representative, DAA, certifier, and program manager must approve revisions to the SSAA. On approval, the necessary changes to the mission, environment, and architecture are documented in the SSAA.

(2) Physical, Personnel, and Management Control Review - The Phase 3 site accreditation evaluation task validated that the site operation of the information system 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.

(3) TEMPEST Evaluation - Periodic TEMPEST and RED-BLACK verification may be required to assure 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.

(4) Compliance Evaluation - This task determines that approved COMSEC 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.

(5) Contingency Plan Maintenance - The contingency plan prepares for emergency response, backup operations, and post-disaster recovery. The plans should, at a minimum, consider natural disasters, enemy actions, or malicious attacks. The availability of critical resources that will support the continuity of operations in an emergency situation must be ensured. The operations and maintenance organizations, with the knowledge and approval of the ISSO, must keep the plans current. This task requires a periodic review of the plans and procedures to ensure they remain current.

(6) Change Management - 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, change management is required to maintain an acceptable level of residual risk.

(a) Accreditation is based on security assumptions that the certified hardware and software of each system to the configuration of the computing environment. Changes in

the information system configuration, operational mission, computing environment, or to the computing environment's configuration may invalidate the security assumptions.

(b) The ISSO and system users must support the system configuration management process. They must be involved in the change 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.

(7) System Security Management - Following the counterpart Phase 3 task, the system management infrastructure should frequently be examined to determine whether it continues to adequately support the maintenance of the environment, mission, and architecture described in the SSAA. Infrastructure components include the security policies, system and security management organizations, security training and awareness, rules of behavior, incident response plan and procedures, virus detection procedures, and the configuration management organization and processes. These components must be kept current and operating in an effective manner. An effective configuration management program is mandatory if an established security posture is to be maintained. The system security management task continues the Phase 3 evaluation of the change control and configuration management practices to determine their ability to preserve the integrity of the security relevant software and hardware.

(8) Risk Management Review - 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.

36. Compliance Validation - Periodic review of the operational system and its computing environment must occur at predefined intervals as defined in the SSAA.[7] The purpose of this activity is to ensure the continued compliance with the security requirements, current threat assessment, and concept of operations as stated and documented in the SSAA. The compliance review should ensure that the contents of the SSAA adequately address the current status of the functional environment in which the IS is operating. The compliance validation tasks should repeat all the applicable Phase 2 and 3 tasks. When compliance validation is conducted the following minimum tasks should be completed:

- Site and Physical Security Validation
- Security Procedures Validation
- System Changes and Related Impact Validation
- System Architecture and System Interfaces Validation
- Management Procedures Validation
- Risk Decisions Validation

[7]OMB, departmental, and agency directives have mandatory recertification and reaccreditation requirements. These requirements must be included in the SSAA, governing security requisites.

SECTION 10 - NIACAP ROLES AND FEDERAL AGENCY MANAGEMENT ORGANIZATION

37. Many organizations within a federal agency have significant roles in contributing to the secure development and operation of their IS[8]. The NIACAP approach allows federal agencies to adapt the NIACAP roles into their respective organizational management structure to best manage the risks to the federal agency's mission throughout the IS life cycle: system development, operation, maintenance, and disposal.

38. The NIACAP management approach integrates existing C&A roles at multiple levels – first at the department or agency level, then at the site and system levels. At the department or agency level, the process should be tailored to the agencies specific needs and management approach. At the site and system levels, the process should be tailored to implement agency requirements and to meet the needs of the specific system and the risks associated with operating that system.

SECTION 11 - DEPARTMENT AND AGENCY LEVEL MANAGEMENT

39. Recognizing the goal of this document is to standardize the C&A process within the federal government, there may remain some instances where specific departments or agencies will need to make modifications to their process or management procedures. The departments of the federal government and their agencies should tailor this process and the roles to meet the specific needs of their agency. The departments and agencies may add additional requirements to assist their management in monitoring the certification process. This could entail, for example, review of SSAAs at department level for all, or specific systems such as those systems that process National Security Information (NSI), large department wide nets, or those systems that pose wide community risk.

SECTION 12 - NIACAP ROLES AND RESPONSIBILITIES

40. The minimum NIACAP roles include 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 the accreditation.

41. The program manager represents the interests of the system throughout its life cycle management (acquisition or maintenance, life cycle schedules, funding responsibility, system operation, system performance, and maintenance). The organization that the program manager represents is determined by the phase in the life cycle of the system.

42. The DAA is an executive 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 business operations of systems under his/her purview. The DAA determines the acceptable level of residual risk for a system.

43. The certifier (and certification team) provides the technical expertise to conduct the certification throughout 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.

44. The operational interests of system users are vested in the user representative. In the NIACAP process, the user representative is concerned with system availability, access,

[8]This description is not an attempt to define the management structure within federal agencies, but instead is provided as an overview to management of the C&A process.

integrity, functionality, and performance in addition to confidentiality as they relate to the mission environment.

45. The NIACAP 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. Figure 6 summarizes the NIACAP roles and the responsibilities.

	Mgmt. Roles	Security Roles		User Roles
Phase	**Program Manager**	**DAA**	**Certifier**	**User Rep.**
Phase 1	• Initiate security dialogue with DAA, certifier, and user representative • Define system schedule and budget • Support NIACAP tailoring and level of effort determination • Define system architecture • Prepare life cycle management plans • Define security architecture • Draft or support drafting the SSAA	• Define accreditation requirements • Obtain threat assessment • Assures the certifier is assigned • Support NIACAP tailoring • Approve the SSAA	• Begin vulnerability and risk assessments • Review threat definition • Lead NIACAP tailoring • Determine level of certification effort • Describe certification team roles and responsibilities • Draft or support drafting the SSAA	• Support NIACAP 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 • Review security Rules of Behavior (ROB) and Security Operating Procedures (SOP) • Report results to the program manager, DAA, and user representative • Determine if system is ready for certification	• Prepare security ROB and SOP • Support certification actions

Phase	Mgmt. Roles	Security Roles		User Roles
	Program Manager	DAA	Certifier	User Rep.
Phase 3	• Support certification activities • Provide access for security test and evaluation • Provide system corrections under configuration management	• Assess vulnerabilities and residual risk • Decides 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 C&A accreditation package • Recommend system 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 • Decide to 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

Figure 6. Summary of NIACAP Roles and Responsibilities

46. Program Manager - The program manager coordinates all aspects of the system from initial concept, through development, to implementation and system maintenance. Figure 7[9] illustrates the role of the program manager in the NIACAP process. The DAA, certifier, and user representative provide advise, information, and guidance to the program manager throughout the NIACAP process.

[9]The blocks under the program manager's control are shown to represent common approaches and do not dictate a requirement for these organizations.

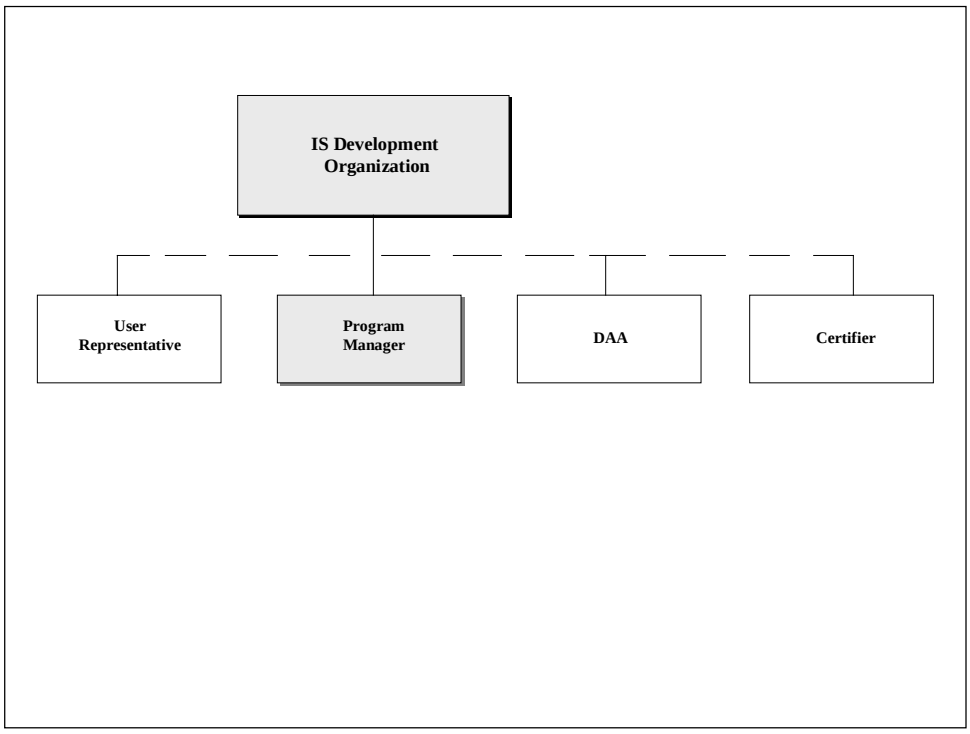


Figure 7. NIACAP Management Relationships[10]

a. 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 NIACAP 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 NIACAP participants informed of life cycle actions, security requirements, and documented user needs.

b. 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.

c. During Phase 3, the program manager ensures that the certification ready system is under configuration management. The DAA, certifier, and user representative validates that the operational environment and system configuration is consistent with the security characteristics reflected in the SSAA.

47. DAA - The DAA is the primary government official responsible for implementing system security.

a. The DAA is 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

[10]Solid lines indicate direct control relationships. Dashed lines indicate coordination relationships.

operational. In reaching these decisions, the DAA is supported by all the documentation provided in the SSAA.

b. The IS may involve multiple DAAs. If so, agreements must be established among the DAAs. These agreements are 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.

48. 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.

49. User Representative - Users are found at all levels of an agency. 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.

Encls:

ANNEX A - SSAA Outline
ANNEX B - References
ANNEX C - Acronyms
ANNEX D - Definitions
ANNEX E - Diagrams

ANNEX A

SSAA OUTLINE

The SSAA is a living document that represents the formal agreement among the DAA, the certifier, the user representative, and the program manager. The SSAA is developed in Phase 1 and updated in each phase as the system development progresses and new information becomes available. At minimum, the SSAA should contain the information in the following sample format:

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 Concept of Operations (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
  - 2.1.4 Personnel
  - 2.1.5 COMSEC
  - 2.1.6 TEMPEST
  - 2.1.7 Maintenance Procedures
  - 2.1.8 Training Plans
- 2.2 Software Development and Maintenance Environment
- 2.3 Threat Description

3.0 SYSTEM ARCHITECTURAL DESCRIPTION
- 3.1 System Description
- 3.2 System Interfaces and External Connections
- 3.3 Data Flow
- 3.4 Accreditation Boundary

4.0 SYSTEM SECURITY REQUIREMENTS
- 4.1 National and Organizational Security Requirements
- 4.2 Governing Security Requisites
- 4.3 Data Security Requirements
- 4.4 Security CONOPS
- 4.5 Network Connection Rules
- 4.6 Configuration and Change Management Requirements
- 4.7 Reaccreditation Requirements

5.0 ORGANIZATIONS AND RESOURCES
- 5.1 Organizations
- 5.2 Resources
- 5.3 Training
- 5.4 Other Supporting Organizations

6.0 NIACAP WORK PLAN
- 6.1 Tailoring Factors
  - 6.1.1 Programmatic Considerations
  - 6.1.2 Security Environment
  - 6.1.3 IT System 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

Appendices should be added to include system C&A documents; optional appendices may be added to meet specific needs. All documentation relevant to the systems' C&A should be included in the SSAA.

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

ANNEX B

REFERENCES

1. Public Law 100-235, "Computer Security Act of 1987," January 8, 1988

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

3. National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 1999

4. An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12 October 1995.

5. Management Accountability and Control, OMB A-123, June 21, 1995.

6. International Standard 15408, Common Criteria, Version 2.0, May 1998.

ANNEX C

ACRONYMS

C&A	Certification and Accreditation
CIO	Chief Information Officer
COMPUSEC	Computer Security
COMSEC	Communication Security
CONOPS	Concept of Operations
COTS	Commercial Off-The-Shelf
CRR	Certification Requirement Review
DAA	Designated Approving Authority
DoD	Department of Defense
EMSEC	Emissions Security
GOTS	Government Off-The-Shelf
IA	Information Assurance
IATO	Interim Approval to Operate
INFOSEC	Information Systems Security
IS	Information System
ISSO	Information Systems Security Officer
IT	Information Technology
NCSC	National Computer Security Center
NDI	Non-Developmental Item
NIACAP	National Information Assurance Certification and Accreditation Process
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National Security Information
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OMB	Office of Management and Budget
OPSEC	Operations Security
ROB	Rules of Behavior
SOP	Security Operating Procedures
SSAA	System Security Authorization Agreement
ST&E	Security Test and Evaluation
TEMPEST	Not an acronym

ANNEX D

DEFINITIONS

The terms used in this document were selected from the NSTISSI No. 4009 definitions when possible. Where new terms are used, the revised or new definitions will be submitted as changes to the NSTISSI No. 4009 in accordance with the guidelines in the NSTISSI No. 4009. Terms that are not defined in the NSTISSI No. 4009 or terms defined differently from the NSTISSI No. 4009 are displayed using italics.

1. Accountability. *Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation.* (NSTISSI No. 4009 – Process allowing auditing of IS activities to be traced to a source that may then be held responsible.)

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 to an acceptable level of risk.

3. *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.*

4. *Acquisition Organization. The government organization responsible for developing a system.*

5. 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 necessary changes in controls, policies, or procedures.

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

7. Certification. Comprehensive evaluation of the technical and nontechnical 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.

8. Certification and Accreditation (C&A) Boundary. The C&A boundary encompasses all those components of the system that are to be accredited by the DAA and excludes a separately accredited system, to which the system is connected.

9. Certification Agent (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 packages.

10. *Certification Requirements Review (CRR). A formal review of the certification requirements.*

11. 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 crypto security, transmission security, emission security, and physical security of COMSEC material.

12. *Computing Environment. The total environment in which an automated information system, network, or a component operates. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationship with other information systems.*

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

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

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

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

17. Designated Approving Authority (DAA, 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.

18. *Developer. The organization that develops the information system.*

19. 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.

20. Environment. Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an IS.

21. *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.*

22. *General Support System. Interconnected set of information resources under the same direct management control which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. [from OMB A-130]*

23. *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, OMB, and federal government departments or agencies. For NSI information, DoD and NSA directives and instructions may apply. Governing security requisites are typically high-level. While their implementation will vary from case to case, these requisites are fundamental and must be addressed.*

24. *Grand Design Program Strategies. Characterized by acquisition, development, and deployment of the total functional capability in a single increment.*

25. *Incremental Program Strategies. Characterized by acquisition, development, and deployment of functionality through a number of clearly defined system increments that stand on their own.*

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

27. *Information Category. The term used to bound information and tie it to an information security policy.*

28. *Information Integrity. The preservation of unaltered states as information is transferred through the system and between components.*

29. *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 departmental systems can be contained in Public Law, Executive Orders, departmental directives, and local regulations. The information security policy lists all the security requirements applicable to specific information.*

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

31. Information Systems Security Officer (ISSO). Person responsible to the DAA for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer.

32. *Information Technology (IT). The hardware, firmware, and software used as part of the information system to perform organization information functions. This definition includes computers, telecommunications, automated information systems, 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.*

33. *Integrator. The organization that integrates the information system components.*

34. 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.

35. *Interim Approval To Operate (IATO). The system does not meet the requirements as stated in the SSAA, but mission criticality mandates the system become operational. The IATO is a temporary approval that may be issued for no more than a one-year period.*

36. *Legacy Information System. An operational information system that existed prior to the implementation of this process.*

37. *Maintainer. The organization that maintains the information system.*

38. *Maintenance Organization. The government organization responsible for the maintenance of an IT system. (Although the actual organization performing maintenance on a system may be a contractor, the maintenance organization is the government organization responsible for the maintenance.)*

39. *Major Application. A major application means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the system in which they operate. [from OMB A-130]*

40. *Mission. The assigned duties to be performed by a Information System.*

41. National Security Information (NSI). Information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure.

42. *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 Unites 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.*

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

44. *Other Program Strategies. Strategies intended to encompass variations and/or combinations of the Grand Design, Incremental, Evolutionary, or other program strategies.*

45. *Program Manager. The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT system.*

46. *Requirements Traceability Matrix (RTM). A matrix, spreadsheet, or table of security requirements used to trace compliance of the requirement to specific software, hardware, or procedures, etc.*

47. Residual Risk. Portion or risks remaining after security measures have been applied.

48. *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.*

49. Risk Assessment. Process of analyzing threats to and vulnerabilities of an IS and the potential impact 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 countermeasures.

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

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

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

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

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

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

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

57. 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.

58. Sensitive Information. Information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of the federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552A (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified 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 (P.L. 100-235).)

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

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

61. *System Security Authorization Agreement (SSAA). The SSAA is a formal agreement among the DAA(s), certifier, IS user representative, and the program manager. It is used throughout the NIACAP to guide actions, and to document decisions, security requirements, certification tailoring and level-of-effort, certification results, certifier's recommendation, and the DAA's approval to operate.*

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

63. 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.

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

65. User. Person or process authorized to access an IS.

66. *User Representative*. *The individual or organization that represents the user or user community in the definition of information system requirements.*

67. Validation. Process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an IS by one or more departments or agencies and their contractors.

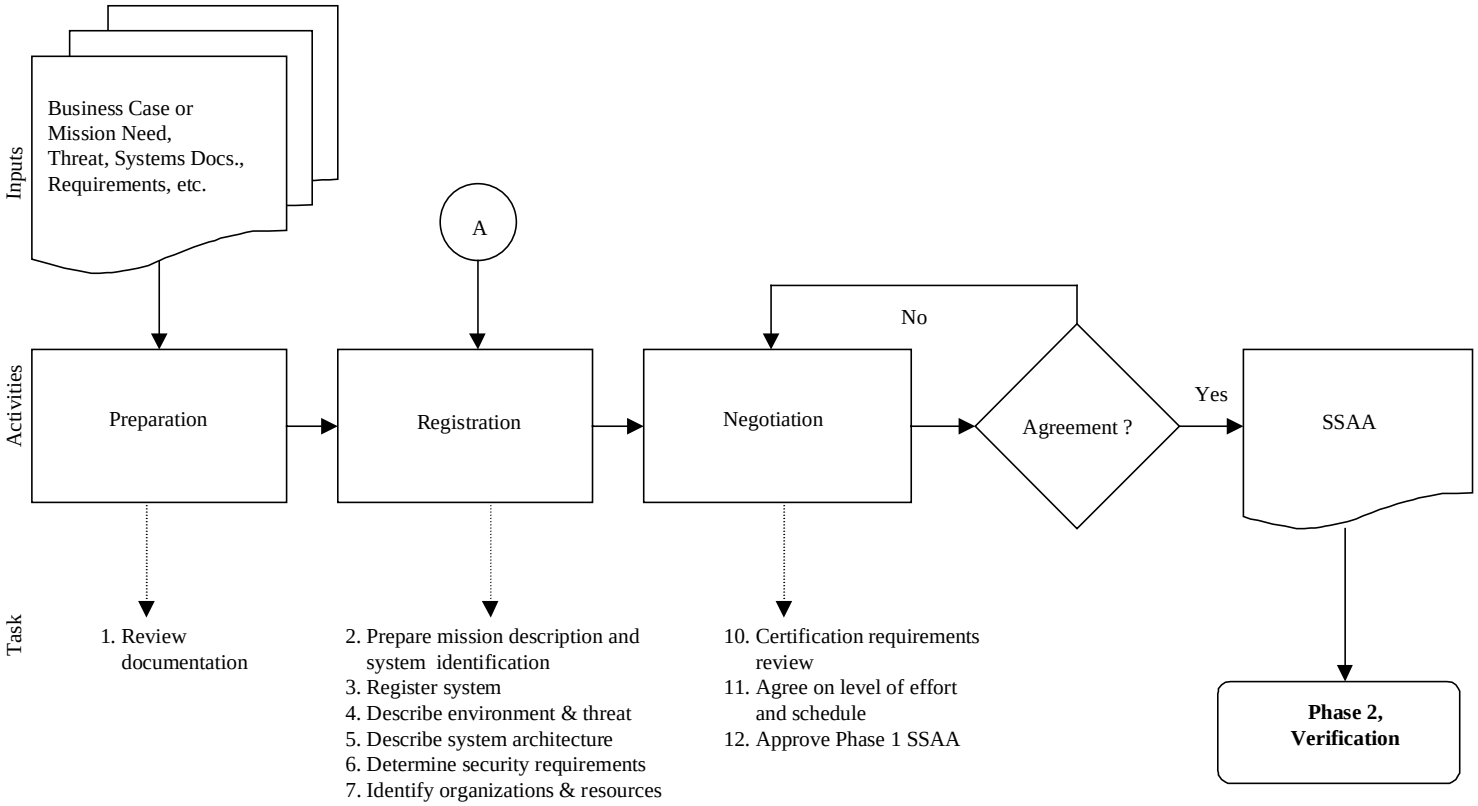
68. Verification. Process of comparing two levels of an IS specification for proper correspondence, e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code.

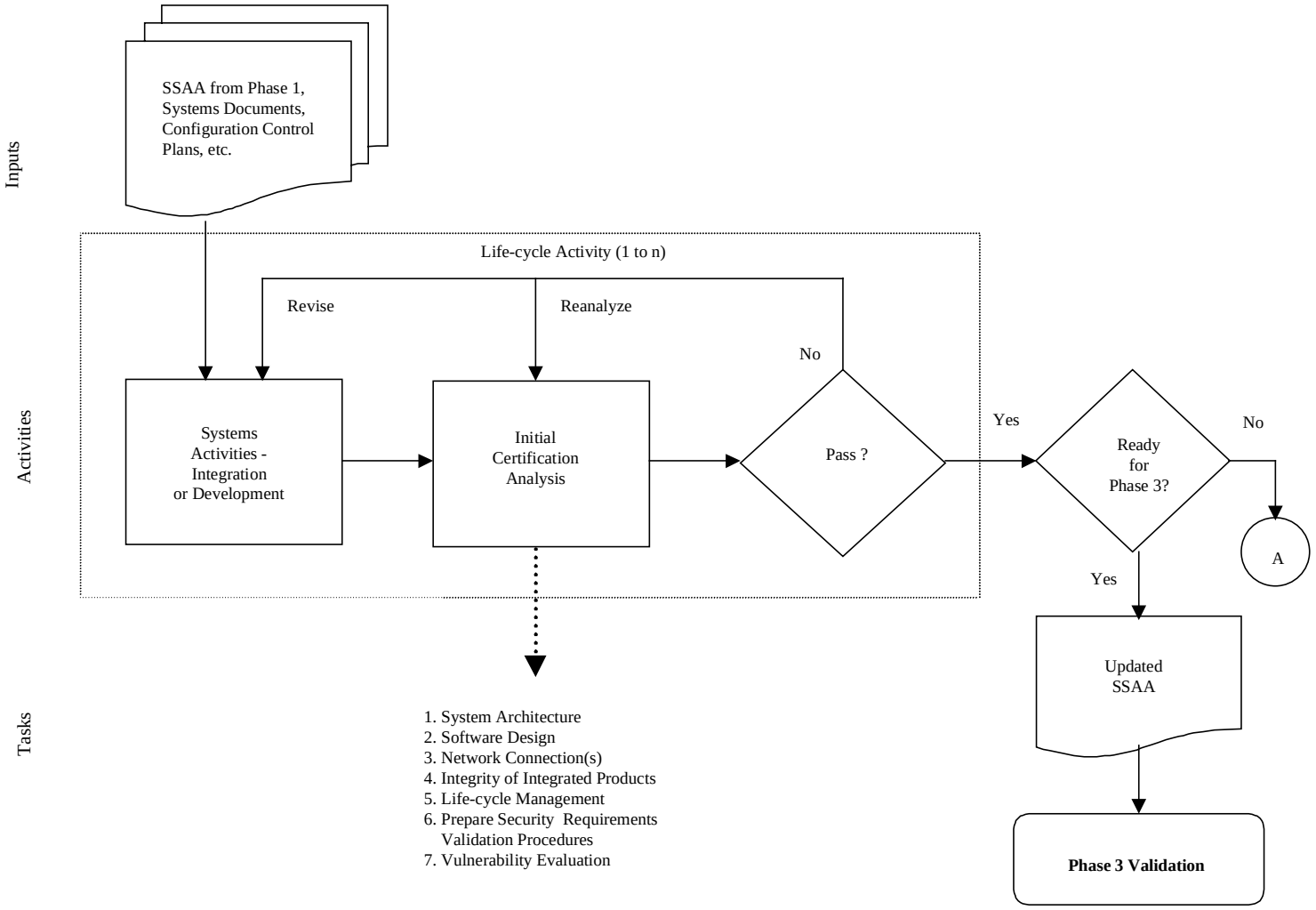
69. Vulnerability. Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.

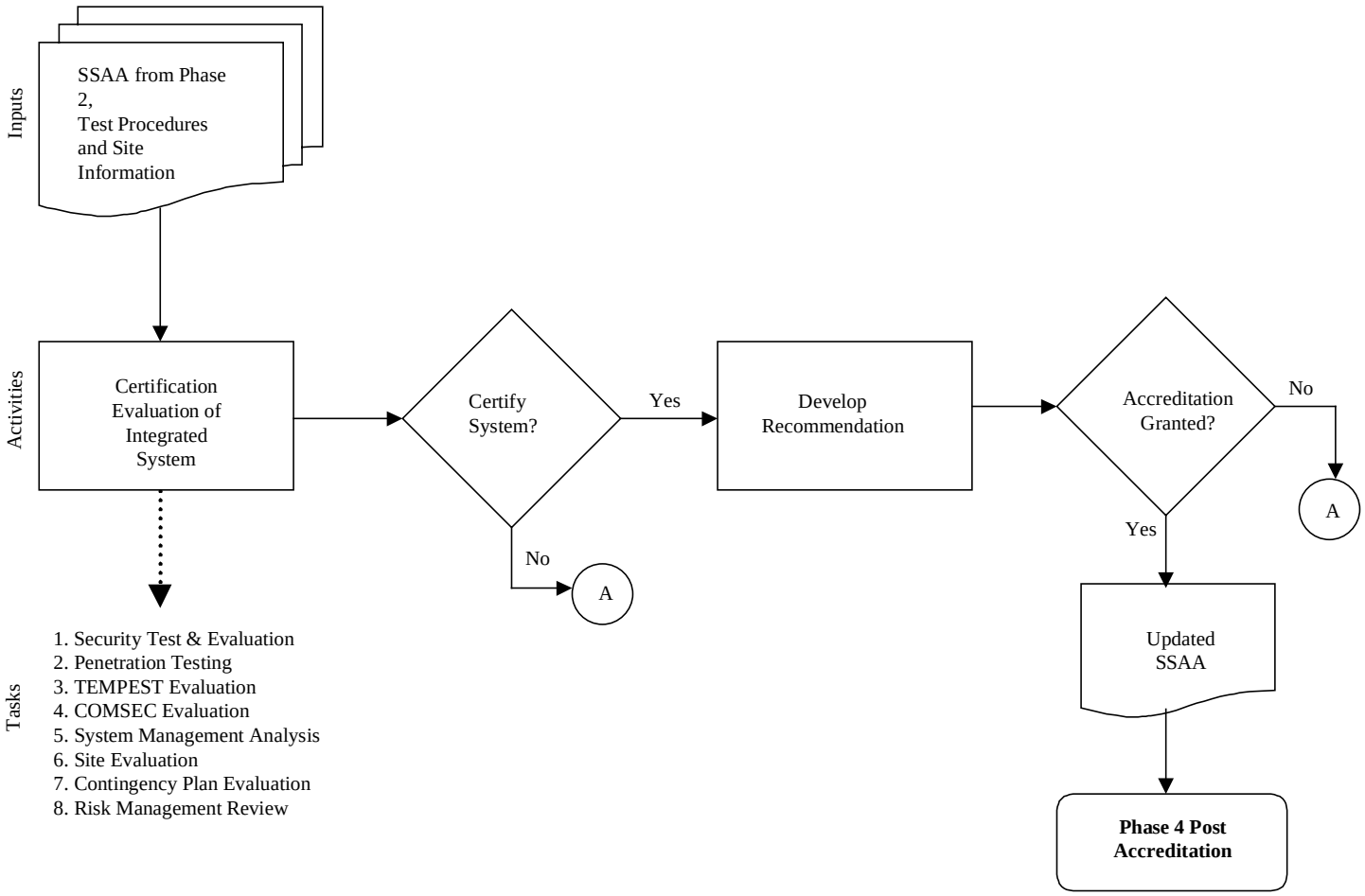
70. Vulnerability Assessment. Systematic examination of an IS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

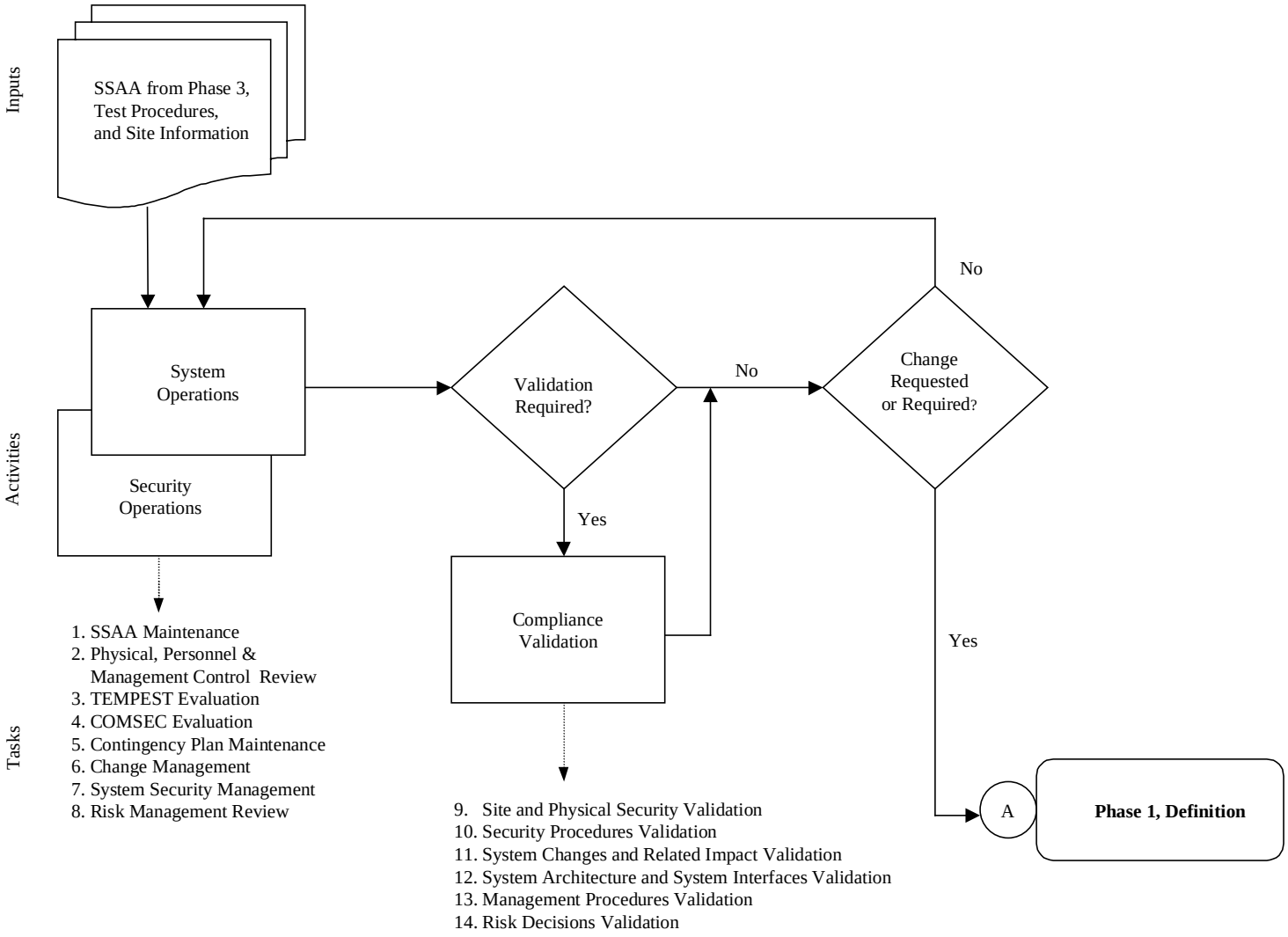
ANNEX E

DIAGRAMS




Inputs
SSAA from Phase 1, Systems Documents, Configuration Control Plans, etc.
Life-cycle Activity (1 to n)
Revise
Reanalyze
No
Activities
Systems Activities - Integration or Development
Initial Certification Analysis
Pass ?
Yes
Ready for Phase 3?
No
A
Yes
Updated SSAA
Phase 3 Validation
Tasks
1. System Architecture
2. Software Design
3. Network Connection(s)
4. Integrity of Integrated Products
5. Life-cycle Management
6. Prepare Security Requirements Validation Procedures
7. Vulnerability Evaluation


Inputs
SSAA from Phase 2,
Test Procedures and Site Information
Activities
Certification Evaluation of Integrated System
Certify System?
Yes
No
A
Develop Recommendation
Accreditation Granted?
No
A
Yes
Updated SSAA
Phase 4 Post Accreditation
Tasks
1. Security Test & Evaluation
2. Penetration Testing
3. TEMPEST Evaluation
4. COMSEC Evaluation
5. System Management Analysis
6. Site Evaluation
7. Contingency Plan Evaluation
8. Risk Management Review


Inputs
SSAA from Phase 3, Test Procedures, and Site Information
Activities
System Operations
Security Operations
Validation Required?
No
Change Requested or Required?
No
Yes
Yes
Compliance Validation
Tasks
1. SSAA Maintenance
2. Physical, Personnel & Management Control Review
3. TEMPEST Evaluation
4. COMSEC Evaluation
5. Contingency Plan Maintenance
6. Change Management
7. System Security Management
8. Risk Management Review
9. Site and Physical Security Validation
10. Security Procedures Validation
11. System Changes and Related Impact Validation
12. System Architecture and System Interfaces Validation
13. Management Procedures Validation
14. Risk Decisions Validation
A
Phase 1, Definition