FISMA reporting and NIST guidelines

A Research Paper

By

Faisal Shirazee, MSNS, CISSP

Executive Summary

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

This paper is for the use of all Information Security Systems Managers (ISSM), Information Security Systems Officers (ISSO), or any other Information Assurance (IA) analysts involved in the C&A process. This guide advocates degrees of assurance as the initial basis for determining the level of effort necessary to complete the C&A. Once the degrees of assurance have been determined, the certification team can then identify the level-of-effort required for verification of the system. The level-of-effort will then define the document package needed for certification and accreditation.

This paper intends to clarify the FISMA reporting requirements and it intends to summarize the NIST 800-37 process of certification and accreditation.

Table of Contents

Section 1: FISMA Reporting and C&A Process

The Federal Information Security Management Act of 2002 (FISMA, Title III, Public Law 107-347, December 17, 2002), provides government-wide requirements for information security, superseding the Government Information Security Reform Act and the Computer Security Act.

Also, according to the Office of Management and Budget (OMB) Circular A-130, Appendix III, the Clinger-Cohen Act supplements the information resources management policies contained in the PRA by establishing a comprehensive approach for executive agencies to improve the acquisition and management of their information resources, by:

1. focusing information resource planning to support their strategic missions;
2. implementing a capital planning and investment control process that links to budget formulation and execution; and
3. rethinking and restructuring the way they do their work before investing in information systems.

Federal agencies are responsible for providing information security protection of information collected or maintained by or on behalf of the agency and information systems used or operated by or on behalf of the agency. NIST has been tasked to develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets. Note: These standards and guidelines do not apply to national security systems.

Federal Agencies are also to give annual and quarterly reports to congress on how to address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to:

a. Annual agency budgets;
b. Information resources management under subchapter 1 of this chapter
c. Information technology management under subtitle III of title 40
d. Program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39
e. Financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101-576) (and the amendments made by that Act)
f. Financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note)
g. Internal accounting and administrative controls under section 3512 of title 31, (known as the `Federal Managers Financial Integrity Act')

FISAM report should include any significant deficiency in a policy, procedure, or practice identified as a material weakness in reporting under section 3512 of title 31.
In addition to the above requirements the report should include the time periods, and the

resources, including budget, staffing, and training, that are necessary to implement the security program and security controls. The description of the security deficiencies should be risk a based description. The FISMA reporting also holds each Federal agency to provide the public with timely notice and opportunities for comment on proposed information security policies and procedure.

Section 2: How to apply NIST guidelines

NIST has been tasked to develop minimum information security requirements (management, operational and technical security controls) for information and information systems in each such category. All three controls are defined in detail in the next few sections of this paper. NIST is also to develop standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of Information security according to a range of risk levels. NIST publication FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" is the guide on how to categorize the Federal Systems.

NIST is also to develop guidelines recommending the types of information and information systems to be included in each category described in FIPS Publication 199 NIST is in the process of producing publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories". A final publication is due some time in the summer of 2004.

Other very important publications are NSIT 800-200 "Minimum Security Controls for Federal Information Systems" and NIST Special Publication 800-53, "Recommended Security Controls for Federal Information". Both of these publications are currently in draft phase. These documents will provide Federal Agencies a common minimum base line for their security controls.

The publication NIST 800-37 (Guide for the Security Certification and Accreditation of Federal Information Systems) is published to guide Federal agencies to a standard Security Certification and Accreditation (C&A) process. All Federal agencies are or will be following these guidelines to certify and accredit their system. NIST 800-37 is a very comprehensive document but it can be overwhelming. I have summarized the steps described in NIST-800-37 that can translate into an easier implementation of NIST 800-37. I am also attaching a check list as an appendix to this document. This appendix A is a checklist to collect information for the Security Plan.

For additional NIST publication please visit the NIST web site at:
http://csrc.nist.gov/publications/nistpubs/index.ht

Section 3: C&A Activities Process Summary

The security certification and accreditation process consists of four distinct phases: (i) an Initiation Phase; (ii) a Security Certification Phase; (iii) a Security Accreditation Phase; and (iv) a Continuous Monitoring Phase. Each phase consists of a set of well-defined tasks and subtasks that are to be carried out, as indicated, by responsible individuals (e.g., the Chief Information Officer, Authorizing Official, Authorizing Official's designated representative, Information Systems Security Manager, Information System Owner, Information Owner, Information Systems Security Officer, Certification Agent, and User Representatives). The security certification and accreditation activities can be applied to an information system at appropriate phases in the system development life cycle. Additionally, the activities can be tailored to apply a level of effort and rigor that is most suitable for the information system undergoing security certification and accreditation

3.1 Phase I – Initiation Phase

The objective of the preparation task is to prepare for security certification and accreditation by reviewing the system security plan and confirming that the contents of the plan are consistent with an initial assessment of risk.

3.1.1 Activity 1: Preparation

The objective of the preparation task is to prepare for security certification and accreditation by reviewing the system security plan and confirming that the contents of the plan are consistent with an initial assessment of risk

3.1.1.1 Task 1.1 - Information System Description

Confirm that the information system has been fully described and documented in the system security plan or an equivalent document.

A typical system description includes:

1. The name of the information system;
2. A unique identifier for the information system
3. The status of the information system with respect to the system development life cycle
4. The name and location of the organization responsible for the information system
5. Contact information for the information system owner or other individuals knowledgeable about the information system
6. Contact information for the individual(s) responsible for the security of the information system
7. The purpose, functions, and capabilities of the information system
8. The types of information processed, stored, and transmitted by the information system
9. The boundary of the information system for operational authorization (or security accreditation)
10. The functional requirements of the information system

11. The applicable laws, directives, policies, regulations, or standards affecting the security of the information and the information system
12. The individuals who use and support the information system (including their organizational affiliations, access rights, privileges, and citizenship, if applicable);
13. The architecture of the information system
14. Hardware and firmware devices (including wireless System and applications software (including mobile code)
15. Network topology; network connection rules for communicating with external information systems, interconnected information systems and unique identifiers for those systems;
16. Encryption techniques used for information processing, transmission, and storage
17. Public key infrastructures, certificate authorities, and certificate practice statements
18. The physical environment in which the information system operates
19. Web protocols and distributed, collaborative computing environments (processes, and applications).

3.1.1.2 Task 1.2 - Security Categorization

Confirm that the security category of the information system has been determined and documented in the system security plan or an equivalent document.

Consult NIST Special Publication 800-59 to confirm that the information system is other than a national security system. For other than national security systems, FIPS 199 establishes three potential impact levels (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing federal information systems.

3.1.1.3 Task 1.3 – Threat Identification

Confirm that potential threats that could exploit information system flaws or weaknesses have been identified and documented in the system security plan, risk assessment, or an equivalent document.

It is important to consider all potential threats that could cause harm to an information system, ultimately affecting the confidentiality, integrity, or availability of the system. Threats can be natural (floods, earthquakes, tornadoes, landslides, avalanches, electrical storms), human (events that are either enabled by or caused by human beings), or environmental (long-term power failures, pollution, chemicals, liquid leakage). Threat information should be coordinated with the Information Systems Security Manager and authorizing official to facilitate reuse and sharing with other information system owners, Organization-wide. The level of effort (i.e., degree of rigor and formality) applied to the threat identification process should be commensurate with the FIPS 199 security category of the information system (i.e., the level of effort increases as the potential impact on agency operations, agency assets, or individuals increases). Threat identification information is typically documented in the risk assessment, which should be included in the system security plan either by reference or as an attachment.

3.1.1.4 Task 1.4 - Vulnerability Assessment

Confirm that flaws or weaknesses in the information system that could be exploited by potential threat sources have been identified and documented in the system security plan, risk assessment, or an equivalent document.

Flaws or weaknesses in an information system that could be exploited by potential threats determine the potential vulnerabilities in that system. Vulnerability identification can be conducted at any phase in the system development life cycle.

If the system is under development, the search for vulnerabilities focuses on the organization's security policies, planned security procedures, system requirement definitions, and developer security product analyses.

If the system is being implemented, the identification of vulnerabilities is expanded to include more specific information, such as the planned security features described in the security design documentation and the results of the developmental security test and evaluation.

If the system is operational, the process of identifying vulnerabilities includes an analysis of the system security controls employed to protect the system. The identification of vulnerabilities can be accomplished in a variety of ways using questionnaires, on-site interviews, document reviews, and automated scanning tools. Vulnerability information associated with system-specific and common security controls should be coordinated with the senior agency information security officer and authorizing officials to facilitate reuse and sharing with other information system owners agency-wide. The level of effort (i.e., degree of rigor and formality) applied to the vulnerability identification process should be commensurate with the FIPS 199 security category of the information system (i.e., the level of effort increases as the potential impact on agency operations, agency assets, or individuals increases).

Vulnerability identification information is typically documented in the risk assessment report, which should be included in the system security plan either by reference or as an attachment.

3.1.1.5 Task 1.5 - Security Control Identification

Confirm that the security controls (either planned or implemented) for the information system have been identified and documented in the system security plan or an equivalent document.

3.1.1.6 Task 1.6 - Initial Risk Determination

Confirm that the risk to the organization's operations, assets, or individuals has been determined and documented in the system security plan, risk assessment, or an equivalent document.

FISMA and OMB Circular A-130, Appendix III, require risk assessments as part of a risk-based approach to determining adequate, cost-effective security for an information system. Assessing Organization-wide risk should be an ongoing activity to ensure that as new threats and vulnerabilities are identified, adequate security controls are implemented. Organization-wide risk is typically documented in the risk assessment, which should be included in the system security plan either by reference or as an attachment.

3.1.2 Activity 2: Notification and Resource Identification

The objective of the notification and resource identification task is to:

1) provide notification to all concerned agency officials as to the impending security certification and accreditation of the information system
2) determine the resources needed to carry out the effort
3) prepare a plan of execution for the certification and accreditation activities indicating the proposed schedule and key milestones

3.1.2.1 Task 2.1 – Notification

The initial notification of key agency officials is an important activity to establish the security certification and accreditation process as an integral part of the system development life cycle. The notification also serves as an early warning to help prepare potential participants for the upcoming tasks that will be necessary to plan, organize, and conduct the security certification and accreditation. In some instances, the authorizing official or Information Systems Security Manager provides the initial notification to the information system owner and other key agency officials. This typically occurs when a specified time period has elapsed and the information system must undergo reaccredidation in accordance with federal or agency policy.

Inform the Information Systems Security Manager, authorizing official, certification agent, user representatives, and other interested agency officials that the information system requires security certification and accreditation support.

3.1.2.2 Task 2.2 – Planning and Resources

Determine the level of effort and resources required for the security certification and accreditation of the information system (including organizations involved) and prepare a plan of execution.

The level of effort required for security certification depends on:

1) the size and complexity of the information system
2) the FIPS 199 security category of the system
3) the security controls employed to protect the system
4) the specific methods and procedures used to assess the security controls in the system to determine the extent to which the controls are implemented correctly

3.1.3 Activity 3 - System Security Plan Analysis, Update, and Acceptance

The objective of the system security plan analysis, update, and acceptance task is to:

1) perform an independent review of the FIPS 199 security categorization
2) obtain an independent analysis of the system security plan

3) update the system security plan as needed based on the results of the independent analysis
4) obtain acceptance of the system security plan by the authorizing official and Information Systems Security Manager prior to conducting an assessment of the security controls in the information system. The completion of this task concludes the Initiation Phase of the security certification and accreditation process.

3.1.3.1Task 3.1 - Security Categorization Review

Review the FIPS 199 security categorization described in the system security plan to determine if the assigned impact values with respect to the potential loss of confidentiality, integrity, and availability are consistent with Organization's actual mission requirements.

FIPS 199 is used as part of Organization's risk management program to help ensure that appropriate security controls are applied to each information system and that the controls are adequately assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements. The review of the security categorization ensures that the information system owner has adequately reflected the importance (including criticality and sensitivity) of the information system in supporting the operations and assets of Organization. Independent review of the security categorization by the certification agent, authorizing official and Information Systems Security Manager is performed as needed to ensure appropriate categorization.

3.1.3.2 Task 3.2 - System Security Plan Analysis

The system security plan provides an overview of the information system security requirements and describes the security controls in place or planned for meeting those requirements. The independent review of the system security plan by the certification agent, authorizing official and Information Systems Security Manager determines if the plan is complete and consistent with the requirements document for the information system. The certification agent, authorizing official, and Information Systems Security Manager also determine, at the level of analysis possible only with available planning or operational documents and information from the risk assessment, if the vulnerabilities in the information system and resulting Organization-wide risk appear to be correct and reasonable. Based on the results of this independent review and analysis, the certification agent, authorizing official and Information Systems Security Manager may recommend changes to the system security plan. Whenever possible, these changes should be reflected in the requirements document for the information system.

3.1.3.3 Task 3.3 - System Security Plan Update

Update the system security plan based on the results of the independent analysis and recommendations of the certification agent, authorizing official and Information Systems Security Manager.

The information system owner reviews the changes recommended by the certification agent, authorizing official, and Information Systems Security Manager and consults with other agency representatives (e.g., information owner, Information Systems Security Officer, or user representatives) prior to making any final modifications to the system security plan. The modifications to the system security plan may include any of the areas described in Task 1 (e.g., adjusting security controls, changing vulnerabilities, or modifying the agency-level risk).

3.1.3.4 Task 3.4 - System Security Plan Acceptance

If the agency-level risk described in the system security plan (or risk assessment) is deemed unacceptable, the authorizing official and Information Systems Security Manager send the plan back to the information system owner for appropriate action. If the Organization-wide risk described in the system security plan (or risk assessment) is deemed acceptable, the authorizing official and Information Systems Security Manager accept the plan. The acceptance of the system security plan and Organization-wide risk assessment represents an important milestone in the security certification and accreditation of the information system. The authorizing official and Information Systems Security Manager, by accepting the system security plan, are agreeing to the set of security controls proposed to meet the security requirements for the information system. This Organization-wide agreement allows the security certification and accreditation process to advance to the next phase (i.e., the actual assessment of the security controls). The acceptance of the system security plan also approves the level of effort and resources required to successfully complete the associated security certification and accreditation activities.

Key Milestones:

- ➢ The following questions should be answered before proceeding to the Security Certification Phase:
  - **Does the FIPS 199 security category of the information system described in the system security plan appear to be correct?**
  - **Have the resources required to successfully complete the security certification and accreditation of the information system been identified and allocated?**
  - **Does the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals described in the system security plan appear to be correct?**
  - **Having decided that the Organization-wide risk appears to be correct, would this risk be acceptable?**

3.2 Phase II: Security Certification

The Security Certification Phase consists of two tasks:
1) Security control assessment and 2) Security certification documentation. The purpose of this phase is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This phase also addresses specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system. Upon successful completion of this phase, the authorizing official will have the information needed from the security certification

to determine the risk to Organization's operations, assets, or individuals—and thus will be able to render an appropriate security accreditation decision for the information system.

3.2.1 Activity 4 - Security Control Assessment

The objective of the security control assessment task is to:

1) Prepare for the assessment of the security controls in the information system
2) Conduct the assessment of the security controls
3) Document the results of the assessment.

Preparation for security assessment involves gathering appropriate planning and supporting materials, system requirements and design documentation, security control implementation evidence, and results from previous security assessments, security reviews, or audits. Preparation also involves developing specific methods and procedures to assess the security controls in the information system.

3.2.1.1 Task 4.1 - Documentation and Supporting Materials

Assemble any documentation and supporting materials necessary for the assessment of the security controls in the information system; if these documents include previous assessments of security controls, review the findings, results, and evidence.

3.2.1.2 Task 4.2 - Methods and Procedures

Select, or develop when needed, appropriate methods and procedures to assess the management, operational, and technical security controls in the information system.

In lieu of developing unique or specialized methods and procedures to assess the security controls in the information system, certification agents should consult NIST Special Publication 800-53A, which provides standardized methods and procedures for assessing the security controls listed in NIST Special Publication 800-53. The certification agent, if so directed by the information system owner, authorizing official, or Information Systems Security Manager, can supplement these assessment methods and procedures. Assessment methods and procedures may need to be created for those security controls employed by Organization that are not contained in NIST Special Publication 800-53. Additionally, assessment methods and procedures may need to be tailored for specific system implementations.

3.2.1.3 Task 4.3 - Security Assessment

Federal Agencies have been instructed to use NSIT 800-26 as the self assessment tool.

Assess the management, operational and technical security controls in the information system using methods and procedures selected or developed.

Security assessment determines the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of the security assessment, including recommendations for correcting any deficiencies in the security controls, are documented in the security assessment report.

3.2.1.4 Task 4.4 - Security Assessment Report

Prepare the final security assessment report. The security assessment report contains:
1) The results of the security assessment (i.e., the determination of the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system)
2) Recommendations for correcting deficiencies in the security controls and reducing or eliminating identified vulnerabilities. The security assessment report is part of the final accreditation package along with the updated system security plan and plan of action and milestones. The security assessment report is the certification agent's statement regarding the security status of the information system.

3.2.2 Activity 5 - Security Certification Documentation

The objective of the security certification documentation task is to: (i) provide the certification findings and recommendations to the information system owner; (ii) update the system security plan as needed; (iii) prepare the plan of action and milestones; and (iv) assemble the accreditation package. The information system owner has an opportunity to reduce or eliminate vulnerabilities in the information system prior to the assembly and compilation of the accreditation package and submission to the authorizing official. This is accomplished by implementing corrective actions recommended by the certification agent. The certification agent should assess any security controls modified, enhanced, or added during this process. The completion of this task concludes the Security Certification Phase.

3.2.2.1 Task 5.1 - Findings and Recommendations

Provide the information system owner with the security assessment report.
The information system owner relies on the security expertise and the technical judgment of the certification agent to:
1) Assess the security controls in the information system
2) Provide specific recommendations on how to correct deficiencies in the controls and reduce or eliminate identified vulnerabilities. The information system owner may choose to act on selected recommendations of the certification agent before the accreditation package is finalized if there are specific opportunities to correct deficiencies in security controls and reduce or eliminate vulnerabilities in the information system. To ensure effective allocation of resources Organization-wide, any actions taken by the information system owner prior to the final accreditation decision should be coordinated with the authorizing official and Information Systems Security Manager. The certification agent assesses any changes made to the security

controls in response to corrective actions by the information system owner and updates the assessment report, as appropriate.

3.2.2.2 Task 5.2 - System Security Plan Update

Update the system security plan (and risk assessment) based on the results of the security assessment and any modifications to the security controls in the information system.

The system security plan should reflect the actual state of the security controls after the security assessment and any modifications by the information system owner in addressing the recommendations for corrective actions from the certification agent. At the completion of the Security Certification Phase, the security plan and risk assessment should contain an accurate list and description of the security controls implemented and a list of identified vulnerabilities (i.e., controls not implemented).

3.2.2.3 Task 5.3 - Plan of Action and Milestones Preparation

Prepare the plan of action and milestones based on the results of the security assessment.

The plan of action and milestones document, one of the three key documents in the security accreditation package, describes actions taken or planned by the information system owner to correct deficiencies in the security controls and to address remaining vulnerabilities in the information system (i.e., reduce, eliminate, or accept the vulnerabilities). The plan of actions and milestones document identifies: (i) the tasks needing to be accomplished; (ii) the resources required to accomplish the elements of the plan; (iii) any milestones in meeting the tasks; and (iv) scheduled completion dates for the milestones.

3.2.2.4 Task 5.4 - Accreditation Package Assembly

Assemble the final security accreditation package and submit to authorizing official.

The information system owner is responsible for the assembly and compilation of the final security accreditation package with inputs from the Information Systems Security Officer and the certification agent. The accreditation package contains:

1) The security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions
2) The plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system
3) The updated system security plan with the latest copy of the risk assessment. Certification agent input to the final accreditation package provides an unbiased and independent view of the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements. The authorizing official will use this information during the Security Accreditation Phase to determine the risk to Organization's operations, assets, or individuals. The accreditation package can be

submitted in either paper or electronic form. The contents of the accreditation package should be protected appropriately in accordance with Organization policy.

Key Milestone:

- The following questions should be answered before proceeding to the Security Accreditation Phase:

  - **To what extent are the security controls in the information system implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system?**

  - **What specific actions have been taken or are planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system?**

3.3 Phase III: Security Accreditation Phase

The Security Accreditation Phase consists of two tasks:
1) Security accreditation decision and 2) Security accreditation documentation. The purpose of this phase is to determine if the remaining known vulnerabilities in the information system (after the implementation of an agreed-upon set of security controls) pose an acceptable level of risk to Organization's operations, assets, or individuals. Upon successful completion of this phase, the information system owner will have one of the following:
1) Authorization to operate the information system
2) An interim authorization to operate the information system under specific terms and conditions
3) Denial of authorization to operate the information system.

3.3.1 Activity 6 - Security Accreditation Decision

The objective of the security accreditation decision task is to: (i) determine the risk to Organization's operations, assets, or individuals; and (ii) determine if the Organization-wide risk is acceptable. The authorizing official, working with information from the information system owner, Information Systems Security Officer, and certification agent produced during the previous phase, has independent confirmation of the identified vulnerabilities in the information system and a list of planned or completed corrective actions to reduce or eliminate those vulnerabilities. It is this information that is used to determine the final risk to Organization and the acceptability of that risk.

3.3.1.1 Task 6.1 - Final Risk Determination

Determine the risk to Organization's operations, assets, or individuals based on the vulnerabilities in the information system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities.

The authorizing official receives the final security accreditation package from the information system owner. The vulnerabilities in the information system confirmed by the certification agent should be assessed to determine how those particular vulnerabilities translate into risk to Organization's operations, assets, or individuals. The authorizing official or designated representative should judge which information system vulnerabilities are of greatest concern to Organization and which vulnerabilities can be tolerated without creating unreasonable Organization-wide risk. The plan of action and milestones (i.e., actions taken or planned to correct deficiencies in the security controls and reduce or eliminate vulnerabilities) submitted by the information system owner should also be considered in determining the risk to Organization. The authorizing official may consult the information system owner, certification agent, or other agency officials before making the final risk determination.

3.3.1.2 Task 6.2 - Risk Acceptability

The authorizing official should consider many factors when deciding if the risk to Organization's operations, assets, or individuals is acceptable. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable accreditation decision. The authorizing official renders an accreditation decision for the information system after reviewing all of the relevant information and, where appropriate, consulting with key agency officials.

If, after assessing the results of the security certification, the authorizing official deems that the Organization-wide risk is acceptable, an authorization to operate is issued. The information system is accredited without any restrictions or limitations on its operation.

If, after assessing the results of the security certification, the authorizing official deems that the Organization-wide risk is unacceptable, but there is an important mission-related need to place the information system into operation, an interim authorization to operate may be issued. The interim authorization to operate is a limited authorization under specific terms and conditions including corrective actions to be taken by the information system owner and a required timeframe for completion of those actions. A detailed plan of action and milestones should be submitted by the information system owner and approved by the authorizing official prior to the interim authorization to operate taking effect. The information system is *not* accredited during the period of limited authorization to operate.

If, after assessing the results of the security certification, the authorizing official deems that the Organization-wide risk is unacceptable, the information system is not authorized for operation and thus is *not* accredited.

3.3.1.3 Activity 7 - Security Accreditation Documentation

The objective of the security accreditation documentation task is to transmit the final security accreditation package to the appropriate individuals and organizations and update the system security plan with the latest information from the accreditation decision. The completion of this task concludes the Security Accreditation Phase of the security certification and accreditation process.

3.3.1.4Task 7.1- Security Accreditation Package Transmission

Provide copies of the final security accreditation package including the accreditation decision letter (in either paper or electronic form), to the information system owner and any other agency officials having an interest (i.e., need to know) in the security of the information system.

3.3.1.5 Task 7.2 - System Security Plan Update

The system security plan should be updated to reflect any changes in the information system resulting from the Security Accreditation Phase. Any conditions set forth in the accreditation decision should also be noted in the plan. It is expected that the changes to the system security plan at this phase in the security certification and accreditation process would be minimal.

Key Milestone:

- ➢ The following questions should be answered before proceeding to the Continuous Monitoring Phase:
    - o **Is this agency-level risk acceptable?**
    - o **How do the known vulnerabilities in the information system translate into agency-level risk— that is, risk to Organization S&T operations, assets, or individuals?**

3.4 Phase IV: Continuous Monitoring Phase

The Continuous Monitoring Phase consists of three tasks:

1) Configuration management and control
2) Security control monitoring
3) Status reporting and documentation.

The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the information system. Reaccredidation may be required because of specific changes to the information system or because federal or Organization policies require periodic reaccredidation of the information system.

3.4.1 Activity 8 - Configuration Management and Control

The objective of the configuration management and control task is to:

1) Document the proposed or actual changes to the information system
2) Determine the impact of proposed or actual changes on the security of the system.

An information system will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the system environment. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.

3.4.1.1 Task 8.1 - Documentation of Information System Changes

An orderly and disciplined approach to managing, controlling, and documenting changes to an information system is critical to the continuous assessment of the security controls that protect the system. It is important to record any relevant information about the specific proposed or actual changes to the hardware, firmware, or software such as version or release numbers, descriptions of new or modified features or capabilities, and security implementation guidance. It is also important to record any changes to the information system environment such as modifications to the physical plant. The information system owner and Information Systems Security Officer should use this information in assessing the potential security impact of the proposed or actual changes to the information system. Significant changes to the information system should not be undertaken prior to assessing the security impact of such changes.

3.4.1.2 Task 8.2 - Security Impact Analysis

Analyze the proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment) to determine the security impact of such changes.

3.4.2 Activity 9 - Security Control Monitoring

The objective of the security control monitoring task is to, select an appropriate set of security controls in the information system to be monitored and assess the designated controls using methods and procedures selected by the information system owner. The continuous monitoring of security controls helps to identify potential security-related problems in the information system that are not identified during the security impact analysis conducted as part of the configuration management and control process.

3.4.2.1 Task 9.1 - Security Control Selection

The criteria established by the information system owner for selecting which security controls will be monitored should reflect Organization's priorities and importance of the information system to the department. For example, certain security controls may be considered more critical than other controls because of the potential impact on the information system if those controls were subverted or found to be ineffective. The security controls being monitored should be reviewed over time to ensure that a representative sample of controls is included in the ongoing security assessments.

3.4.2.2 Task 9.2 - Selected Security Control Assessment

Assess an agreed-upon set of security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

> The continuous monitoring of security controls can be accomplished in a variety of ways including security reviews, self-assessments, security testing and evaluation, or audits.

3.4.3 Activity 10 - Status Reporting and Documentation

The objective of the status reporting and documentation task is to:

1. Update the system security plan to reflect the proposed or actual changes to the information system
2. Update the plan of action and milestones based on the activities carried out during the continuous monitoring phase
3. Report the security status of the information system to the authorizing official and Information Systems Security Manager.

The information in the security status reports (typically conveyed through updated plans of action and milestones) should be used to determine the need for security reaccredidation and to satisfy FISMA reporting requirements.

3.4.3.1 Task 10.1 - System Security Plan Update

Update the system security plan based on the documented changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.

3.4.3.2 Task 10.2 - Plan of Action and Milestones Update

Update the plan of action and milestones based on the documented changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.

3.4.3.3 Task 10.3 - Status Reporting

Report the security status of the information system to the authorizing official and Information Systems Security Manager.

The security status report (which can be submitted in the form of an updated plan of action and milestones) should describe the continuous monitoring activities employed by the information system owner. The security status report addresses vulnerabilities in the information system discovered during the security certification, security impact analysis, and security control monitoring and how the information system owner intends to address those vulnerabilities (i.e., reduce, eliminate, or accept the vulnerabilities). The authorizing official and the Information Systems Security Manager should use the security status reports to determine if a security re-accreditation is necessary.

Key Milestone:

- The following questions should be answered before reinitiating the certification and accreditation process:

    - **Have any changes to the information system affected the security controls in the system or introduced new vulnerabilities into the system?**

    - **If so, has the Organization-wide risk—that is, the risk to Organization's operations, assets, or individuals been affected? Or**

    - Has a specified time period passed requiring the information system to be reauthorized in accordance with federal or Organization policy?

Appendix A. A Checklist for SP

Index	SSP Requirement	Response	Score	Comments
System Identification				
1	Provide system name, title, or unique identifier.			
2	Categorize the system as a General Support System (GSS) or Major Application (MA). (Use NSIT 800-199 to categorize your system)			
3	Is the SSP's classification or sensitivity clearly marked?			
4	Provide the name of the organization responsible for the system, to include an address and other contact information.			
5	List the name, title, organization, telephone number, e-mail, of the person(s) designated to be the point(s) of contact of the system including system owner, project manager, etc.			
6	List the name, title, organization, telephone number, e-mail, of the person(s) designated to be responsible for the security of the system.			
7	Are there appointment letters?			
8	Describe the operational status of the system, such as operational, under development, undergoing a major modification, etc.			
9	Describe the function and purpose of the system.			
10	If GSS, are MAs supported listed?			
11	Describe system environment including boundaries and any special security concerns (e.g., Internet connection), hardware, software, and communications resources.			
System Interconnection and Data Sharing				
12	Provide a list of all systems to which the system under review is connected - to include the Internet - or with which it shares information.			

Index	SSP Requirement	Response	Score	Comments
13	Provide names, unique identifiers and the owner organization for all systems to which the system under review is connected or with which it shares information.			
14	Describe system interconnection and information sharing with other systems including a Memorandum of Understanding or Agreement (MOU/MOA) for each interface.			
System Sensitivity				
15	List laws, regulations, and policies affecting the system.			
16	Describe system’s criticality (mission critical, mission important, or mission supportive).			
17	Describe system’s sensitivity (confidentiality, integrity, and availability) of the information processed, stored, or transmitted by the system, and assess rates for each (low, medium, or high).			
Management Controls				
Risk Management				
18	Describes the risk assessment methodology used.			
19	Does the risk assessment methodology identify threats, vulnerabilities, and additional security controls required / implemented to mitigate risks?			
20	If no risk assessment has been performed, does the SSP include a milestone date for its completion?			
21	If last risk assessment was performed more than three years ago or if there have been major changes to the system, does SSP include a milestone date for completion of follow-up risk assessment?			
Review of Security Controls				
22	Include a description of the type of security controls review (i.e. OIG audit, self-assessment, etc.) conducted for the system in the last three years.			
23	Include a summary of major findings (to include material weaknesses) for the security controls reviews conducted.			

Index	SSP Requirement	Response	Score	Comments
Rules of Behavior				
23	Describe rules of behavior for the system.			
System Lifecycle				
24	Describe how planning for security is handled throughout each phase of the System Development Life Cycle (SDLC).			
25	Is the system's SDLC phase identified?			
If the system is in the development/acquisition phase, does the System Security Plan contain the following info				
26	Security requirements identified during the design phase.			
27	Security controls test procedures developed before procurement.			
28	Solicitation documentation includes/d security requirements and evaluation/test procedures.			
If the system is in the implementation phase, does the SSP contain the following information				
29	Description of when and who conducted design reviews and system tests.			
30	Testing schedule and procedures for controls implemented after initial testing and acceptance.			
31	Identifies/references test procedures documentation.			
32	Describe whether such documentation is maintained up-to-date.			
If the system is in the operational phase, does the SSP contain the following information				
33	The security operations and administration to include information pertaining to backup procedures, training for users and administrators, management of cryptographic keys, maintenance of user and administrative privileges, and updating security.			
34	Description of the process for ensuring operation assurance (I.e. if C&A is the process for operational assurance, then reference the authorize processing section or appropriate accreditation documentation).			
35	Detailed auditing processes used to maintain system operational assurance.			

Index	SSP Requirement	Response	Score	Comments
If the system is in the disposal phase, does the SSP provide the following information				
36	The requirements for and procedures secure transfer and/or long-term storage of data. (Note: The requirements comes from the data owner or the organization)			
37	Requirements and procedures for media sanitization. Again, The requirements comes from the data owner or the organization			
Authorize Processing				
38	References or contains information pertaining to system certification and accreditation.			
If processing authorized, does C&A documentation include the following information				
39	Completed technical and/or security evaluation. This step could wait till the end of the second phase of the NIST 800-37 process.			
40	Completed risk assessment (RA). The RA could be of number of formats. Please see the NIST 800-37 and NIST 800-30 for further guidance. In a nutshell a RA should list out all the vulnerabilities associated with your system or application, identify the threat associated with them and a risk based decision on realization of those vulnerabilities.			
41	Established rules of behavior that have been signed by all users.			
42	Completed and tested contingency plan.			
43	Statement certifying that system meets all applicable federal laws, regulations, policies, guidelines and standards.			
44	Statement certifying that stated safeguards are in place, appears adequate for the system, and operates as intended.			
Operational Controls				
Personnel Security				
45	Lists sensitivity levels for each position. By position it means the job title.			
46	Clearly describe the background screening process			

Index	SSP Requirement	Response	Score	Comments
47	Thoroughly write out the access controls for individuals who have been granted access prior to background check			
48	Have in depth description of how user access is restricted (least privilege) to data files, to processing capability, or to peripherals and type of access (e.g., read, write, execute, delete) to the minimum necessary to perform the job			
49	Describes how critical functions are divided among different individuals (separation of duties) to ensure that no individual has all necessary authority or information access which could result in fraudulent activity			
50	State he process for requesting, establishing, issuing, and closing user accounts			
Physical and Environmental Security				
51	What are the access controls restricting the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network (LAN) server?			
52	Lists the fire safety procedures of the building that house the systems			
53	How support utilities, such as, electric power, heating and air conditioning, water sewage and other utilities are verified for operability?			
54	Are the controls to prevent data interception from direct observation, interception of data transmission and electromagnetic interception listed out clearly?			
Production and Input/Output Controls				
55	Detail the help desk support which can respond to security incidents in a timely manner			
56	Write out or point out in the respective document the procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information			

Index	SSP Requirement	Response	Score	Comments
57	Describes procedures to ensure that authorized users pick up, receive, or deliver input and output information and media. This process could be part of SP or there could be a pointer reference to another appropriate document.			
58	Consult with the privacy office and ensure that internal/external labeling for appropriate sensitivity (e.g., Privacy Act, Proprietary) are used according to the organizational policy and associated privacy laws.			
59	List or point to an appropriate document, which describes procedures and controls used for transporting or mailing media or printed output			
Contingency Planning – See B-2.7				
60	Include emergency, backup, and contingency procedures.			
61	Lists contingency planning tests, frequency, and totals.			
Software Maintenance Controls				
62	Describes how application or software was developed (in-house or under contract)			
63	List the ownership of software. Who ultimately owns the application? Usually a person but could be a title of an organization.			
64	If the application software is copyrighted commercial off-the-self product or shareware or if the software is sufficiently licensed, write out either scenarios clearly.			
65	Give a detail description of the change control process in place for the application or software or point to an appropriate document.			
Data Integrity Controls				
66	Give detail description of how data is protected from virus			
67	What mechanisms are in place to protect data from unlawful modification? List them out clearly			
68	Describes integrity controls used within the system			

Index	SSP Requirement	Response	Score	Comments
69	If intrusion detection tools are installed on the system, give detail description of its installation and usage.			
70	Describes how system performance monitoring are used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes			
71	List how message authentication is used in the application to ensure that the sender of a message is known and that the message has not been altered during transmission			
System Documentation				
72	List all the documentation maintained for the system. Basically, list all the relevant document to the SP			
Security Awareness and Training – See B-2.6				
73	Include security training curriculum, frequency, and totals.			
74	List any specialized training for security personnel (ISSO, ISSM, etc.), system administrators, etc.			
Technical Controls				
Identification and Authentication				
75	Thoroughly describe the method of user authentication (password, token and biometrics)			
76	List the password system used, including allowable character set. List the organizational requirement of password length.			
77	Either point to or write detail procedures for training users and the materials covered.			
78	Describes the frequency of password changes and how password changes are enforced			
79	If biometrics controls are used, describe them and explain how they are implemented			
80	Again, if token controls are used on the system give a detail description of them and how they are implemented			
81	List the level of enforcement of the access control mechanism (network, operating system, and application)			

Index	SSP Requirement	Response	Score	Comments
82	Describe how the access control mechanism supports individual accountability and audit trails (e.g. passwords are associated with a user identifier that is assigned to a single individual)			
83	Thoroughly describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text password)			
84	Include the lock out criteria. For example, number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and the actions taken when the limit is exceeded			
85	If applicable, detail the use of electronic signatures and the security controls provided			
86	List the policy and the implementation of cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction and archiving			
Logical Access Controls				
87	Clearly state, how separation of duties is enforced to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion			
88	Describe the application's capability to establish an Access Controls List or register of the users and the type of access they are permitted			
89	Give detail description of how Access Control List is maintained			
90	Thoroughly define how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their application			

Index	SSP Requirement	Response	Score	Comments
91	List how often Access Control Lists are reviewed to identify and remove users who have left organization or whose duties no longer require access to the application			
92	Describes controls to detect unauthorized transaction attempts by authorized and/or unauthorized users			
93	Point out or describe the policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users			
94	Clearly define, after what period of user inactivity the system automatically blanks associated display screens and incase of an application after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password to reconnect.			
95	Explain how encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures			
96	List what other hardware or technical control are used to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities if the system is connected to the Internet or other wide area network(s).			
97	Describes any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required.			
98	Evaluate and determine whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions.			
99	If applicable, describe how host-based authentication is used.			

Index	SSP Requirement	Response	Score	Comments
Public Access Controls				
If applicable, does the SSP provide a description of the public access controls to include the following information				
100	I&A controls used, where applicable.			
101	Access controls used to limit user access and privileges.			
102	Controls to prevent modification of data.			
103	Digital Signatures.			
104	Segregation of system for public access.			
105	Generation of data copies for systems accessed by the public.			
106	Controls to prohibit public access to live databases.			
107	Controls to ensure information distributed to public is virus-free.			
108	Audit trails and user confidentiality.			
109	System and data availability.			
110	Legal considerations.			
Auditing				
111	Explain how audit trail are used to support accountability by providing a trace of user actions			
112	Clearly define and write out the three Ws of auditing. That is, who, when, and why accessed the information of your system.			
113	Describes how audit trails are designed and implemented to record appropriate information to assist in intrusion detection			
114	If applicable, describe how audit trials used as online tools to help identify problems other than intrusions as they occur			
115	Provide supporting argument that implemented audit trails are sufficient to establish what events occurred and who (or what) caused them.			
116	Clearly provide explanation on how access to audit logs are restricted			
117	Describes how separation of duties between security personnel who administer the access control function and those who administer the audit trial are used and enforced			

Index	SSP Requirement	Response	Score	Comments
118	List how frequently audit trails are reviewed and whether there are review guidelines			
119	Explain how the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.			
120	If audit analysis tools are used, describes how those Audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, are used in a real-time or near real-time fashion			

Appendix B: ACRONYMS

AIS	automated information system
AFR	Air Force Regulation
CA	certification authority
C&A	certification and accreditation
CAP	connection approval process
CCB	Configuration Control Board
CI	configuration item
CM	configuration management
COMPUSEC	computer security
COMSEC	communications security
CONOPS	concept of operations
COTS	commercial-off-the-shelf
CPU	central processing unit
CTTA	Certified TEMPEST Technical Authority
DAC	discretionary access control
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DODD	Department of Defense Directive
DT&E	development test & evaluation
DTLS	Descriptive top-level specification
ECP	engineering change proposal
EPL	evaluated products list
FCA	functional configuration audit
FER	final evaluation report
FIPS	federal Information Processing Standard
FSRS	functional security requirements specification
FTLS	formal top-level specification
GOTS	Government-off-the-shelf
HVAC	heating/ventilation/air conditioning
I&A	Identification and authentication
INFOSEC	information systems security
I/O	input/output
IOC	initial operational capability
ISSO	Information Systems Security Officer
ISSWG	information systems security working group
IV&V	independent validation and verification
LAN	local area network
MAC	mandatory access control
MOA	memorandum of agreement
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency

NSO	network security officer
OI	operating instruction
OMB	Office of Management and Budget
OPSEC	operations security
OT&E	operational test and evaluation
PC	personal computer
PCA	physical configuration audit
PM	program manager
RFP	request for proposal
ROM	rough order of magnitude
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SFUG	security features user’ s guide
SOW	statement of work
ST&E	security test and evaluation
TASO	terminal area security officer
TCB	trusted computing base
TFM	trusted computing base
TRANSEC	transmission security
TS	top secret
WAN	wide area network

REFERENCES

1) National Institute Standard and Technology (NIST), Guide for the Security Certification and Accreditation of Federal Information Systems, Version 1.2, May 24, 2004.

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

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

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

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

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

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

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

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

10) Office of the Auditor General of Canada: Information Sensitivity and Security Assessment for Computer Information Holdings.

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

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

13) Arca Systems, Inc. Guidance for Developing a Certification and Accreditation Plan (draft), 28 April 1993.

14) Information Systems Security Organization, Information System Security Policy Guideline (draft), 1 April 1993.

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

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

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

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

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

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

21) U.S. General Services Administration, Office of Technical Assistance: Information Technology Installation Security. Defense Logistics Agency (DLA) Regulation No. 5200.17, 9 October 1991. Department of the Navy Automated Information Systems Security Guidelines.

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

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

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