Department of Health & Human Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-13-27
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS INFORMATION SECURITY (IS) CERTIFICATION AND ACCREDITATION (C&A) PROGRAM PROCEDURES

Version 2.0 FINAL
October 10, 2007

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1. OVERVIEW

The *CMS Information Security (IS) Certification & Accreditation (C&A) Program Procedures* supersedes both the *CMS Information Security (IS) Certification & Accreditation (C&A) Methodology, version 1.0, dated May 12, 2005* and the *CMS Information Security (IS) Certification & Accreditation (C&A) Procedures, version 1.0, dated May 12, 2005.* This procedure is promulgated under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004. Federal law requires the Centers for Medicare & Medicaid Services (CMS) to implement a risk-based program for cost-effective IS. All business processes operate with some level of risk, and one of the most effective ways to protect these business processes is through the implementation of effective internal security controls, risk evaluation, and risk management.

To manage a risk-based IS program, Business Owners are responsible for executing the processes defined in the CMS IS C&A Program, such as:

- *CMS Information Security Risk Assessment Procedure*
- *CMS System Security Plans (SSP)*
- *CMS Information Security Contingency Plan Procedures*
- *CMS Information Security Testing Approach*
- Identify vulnerabilities and risk resulting from system implementation
- Authorize, in writing by the Chief Information Officer (CIO), the operation of an information system prior to full implementation and whenever significant changes in the system are affected

These responsibilities form the foundation for the CMS IS C&A Program, which is a critical component of the entire CMS System Development Life Cycle (SDLC)[1], "Framework". All CMS IS Program documents are available at http://www.cms.hhs.gov/informationsecurity/ .

For clarification purposes, C&A Program and the C&A Program procedures are defined below:

- The C&A Program defines how certification activities and the accreditation decision are integrated into the SDLC.
- The C&A Program procedures provide the Business Owner and System Developer / Maintainer with basic instructions for preparing the necessary documentation to demonstrate and to validate that appropriate security controls exist to safeguard the system. The process is also expected to provide a guideline for the accreditation decision-maker on how to evaluate the system certification materials.

[1] The Centers for Medicare & Medicaid Services (CMS) Integrated IT Investment & System Life Cycle Framework ("Framework") http://www.cms.hhs.gov/SystemLifecycleFramework/

1.2.SCOPE

The C&A Program Procedures cover six (6) distinct phases to form a continuous security management practice for all CMS systems/applications. Business Owners of systems that are already in production, or are currently accredited, may only need to address the final phase of the C&A Program, which defines activities performed during maintenance of the system and for periodic re-accreditation.

Each phase of the C&A Program has individual objectives, tasks, and artifacts that are required. The completion of each successive phase depends upon the output of the preceding phase. To manage the C&A Program effectively and efficiently, individual tasks, responsibilities, and expectations are defined within each phase. The C&A phases are structured to integrate the C&A Program within the existing CMS "Framework."

1.3.ROLES & RESPONSIBILITIES

The following roles are responsible for various tasks, assignments, and deliverables throughout the C&A Program:

Table 1: Roles and Responsibilities

Role	Responsibility
CHIEF INFORMATION OFFICER (CIO)	• Maintain the overall responsibility and authority for the CMS C&A Program • Authorize system operation by reviewing the C&A package and signing the CMS IS Accreditation or a conditional Authority to Operate (ATO) • Appoint Designated Approving Authority (DAA)
DESIGNATED APPROVING AUTHORITY (DAA)	• NOTE: At this time, CMS has chosen not to appoint DAAs
CHIEF INFORMATION SECURITY OFFICER (CISO)	• Appointed by the CIO to implement the CMS IS C&A Program and manage the C&A Program tasks • Consults on authorizing decisions concerning CMS IS policies, standards and procedures • Reviews the C&A package • Makes recommendation to the CIO regarding accreditation decision
COMPONENT INFORMATION SYSTEM SECURITY OFFICER (ISSO)/SYSTEM SECURITY OFFICER (SSO)	• Collaborates with the Business Owner and the System Developer / Maintainer to ensure internal system controls conform to CMS IS policy and standards, and fulfill C&A requirements • Provides technical input to the Corrective Action Plans (CAPs) • Periodically validates the internal system controls to ensure implementation in accordance with the system documentation • Certifies that the implemented internal system controls are adequate to meet CMS policy and C&A Program requirements by signing and approving the Certification package

Role	Responsibility
BUSINESS[2] OWNER	• Responsible for IS of the assigned system/application and all related IS artifacts • Prepares the C&A package including supporting documentation • Certifies the implemented internal system controls are adequate to meet CMS policy, standards and C&A Program requirements by signing and approving the Certification package • Serves as liaison between the CISO, the System Developer / Maintainer and the Component ISSO / SSO • Selects the C&A Evaluator and oversees the Evaluator's performance • Correlates internal and external audit information into the C&A Program • Creates and executes CAPs in collaboration with the System Developer/Maintainer, the Component ISSO / SSO, and the CISO
SYSTEM DEVELOPER / MAINTAINER	• Conducts the IS RA and provides technical input for the SSP, IS RA, CP and the CAPs • Incorporates internal controls into the system in consultation with the Business Owner • Enhances/modifies internal controls based on CAPs
C&A EVALUATOR	• Coordinates C&A/Security Test & Evaluation (ST&E) planning with Business Owner and System Developer / Maintainer, including but not limited to time line and resource requirements • Conducts the ST&E specific tasks, including but not limited to updating the ST&E report • Assists Business Owner by developing accreditation recommendations for the CIO

2. CERTIFICATION AND ACCREDITATION PROGRAM

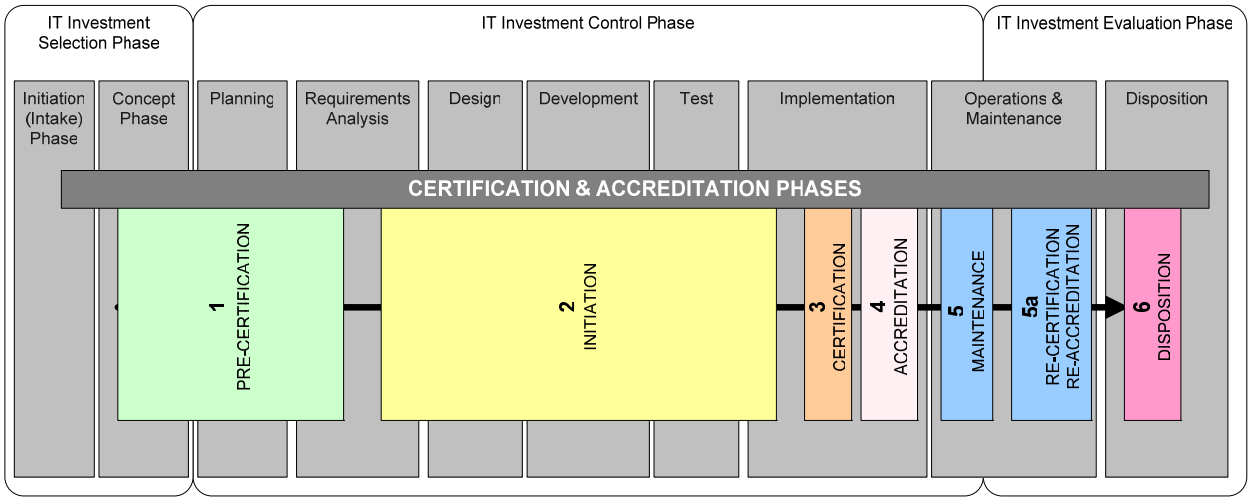
The C&A Program consists of six (6) distinct phases to form a continuous security management practice. Each phase within the C&A Program has individual objectives and tasks, and completion of each successive phase depends upon the output of the preceding phase. To manage the C&A Program effectively and efficiently; individual tasks, responsibilities, and expectations are defined within each phase. Although each phase is depicted to be distinct and sequential, in practice some activities may be implemented in rapid succession, e.g. in rapid application development situations.

The C&A Program is a set of methodological processes and activities that must correlate with the development of the General Support System (GSS), Major Application (MA), or Application.

Figure 1 below shows the C&A phases involved in the C&A Program and the corresponding CMS "Framework" phases.

[2] The Business Owner is equivalent to NIST and Department usage of Information System Owner.

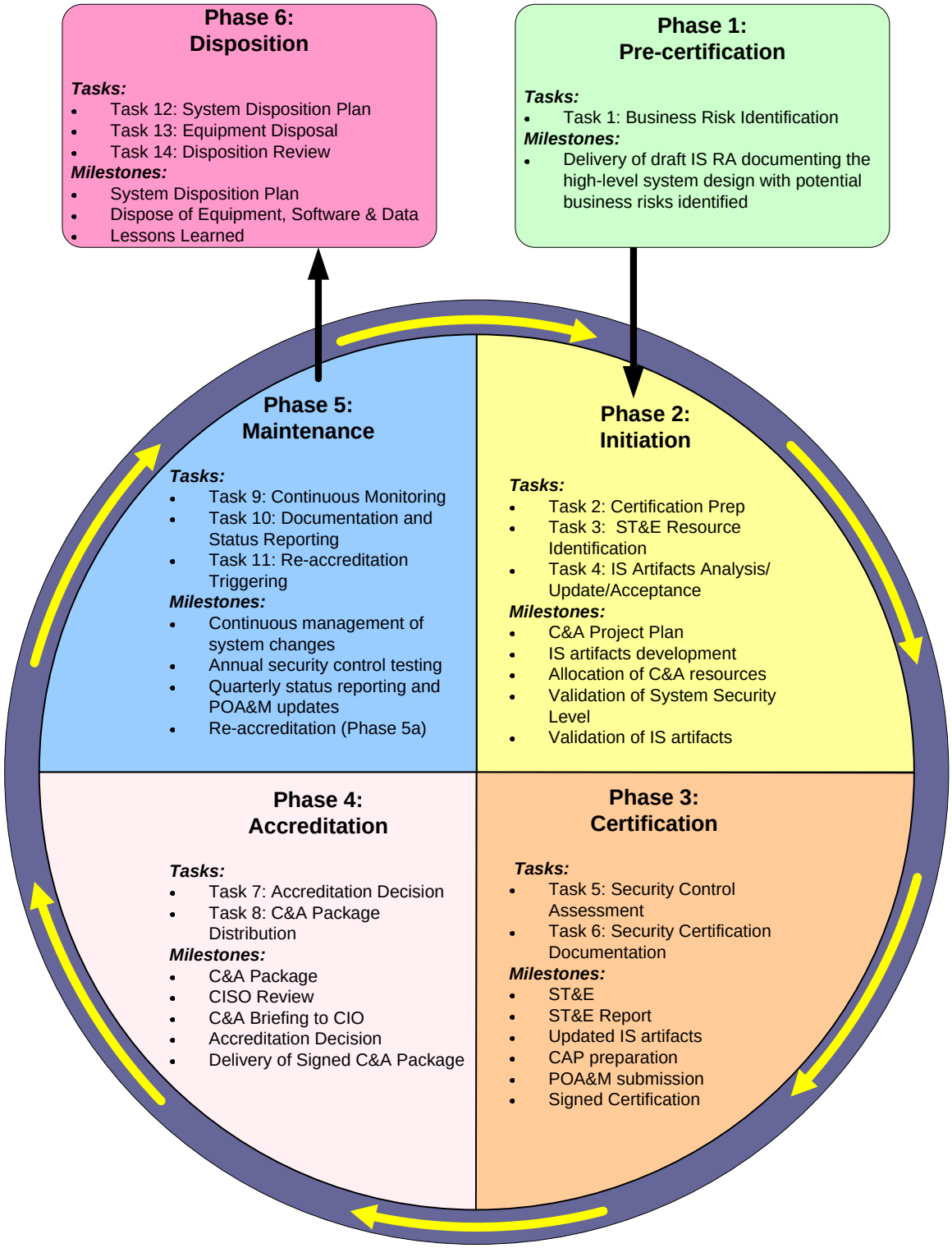
Figure 1: CMS "Framework" and C&A Phases



The CMS "Framework" diagram, Figure 1, shows how the C&A Program phases integrate into the CMS SDLC. Investment control, SDLC and C&A phases are correlated to provide an overall understanding of how C&A corresponds to the overall implementation of a system within the CMS environment.

C&A is a recurring process. As indicated in Figure 2, the C&A Program diagram, the Business Owner and the System Developer / Maintainer must continually update the system documentation as changes are implemented over time. Continuous Maintenance activities can affect the effectiveness of the system security controls. As such, the security controls must be periodically evaluated until the system is disposed.

Figure 2: CMS C&A Program



3. IMPLEMENTATION APPROACH

3.1. PHASE 1 - PRE-CERTIFICATION

The objective of the Pre-Certification Phase is to integrate the system into the CMS C&A Program as required by NIST SP 800-37. The Pre-Certification Phase includes the initiation of the IS RA, including business risks.

TASK 1: BUSINESS RISK IDENTIFICATION
The objective of this task is to:

- Budget for C&A activities
- Identify business risks, roles and responsibilities
- Describe the initial high-level design considerations for IS

This will serve as the foundation for the subsequent C&A activities.

The following activities should take place during this task:
The Business Owner shall include adequate resource requests for C&A activities as part of their IT Investment request and:

- Initiate development of the IS RA by completing as much of Section 1 as possible
- Ensure the completion of the business risks portion of the IS RA (during the Concept phase of the CMS "Framework")

The process described in the following four (4) phases directs the CMS Business Owner and System Developer/Maintainer in implementing and managing the required C&A Program for an information system.

3.2. PHASE 2 - INITIATION

This phase establishes the processes necessary for analyzing and determining the systems security requirements (i.e., controls), assessing the risks and vulnerabilities to CMS information and information systems and accurately documenting them in the SSP and IS RA accordingly. The Initiation Phase consists of three tasks: (i) preparation; (ii) notification and resource identification; and (iii) security artifacts' analysis, update, and acceptance.

TASK 2: CERTIFICATION PREPARATION
The objectives of this task are:

- Create C&A project plan indicating the proposed schedule and key milestones
- Confirm that the business risks are realistic projections
- Continue development of the IS RA and initiate development of the SSP through the Development Phase.
- Update the IS RA and SSP during the Testing Phase of the "Framework"
- Define the IS requirements (i.e. controls) necessary to protect CMS information and information systems against potential risks, both business and technical. **NOTE**: The primary driver for the level of controls is derived from the sensitivity of the data as defined in the *CMS System Security Levels*.

The Business Owner shall ensure that the following activities take place during this task:

- Oversee the System Developer/Maintainer C&A activities
- In collaboration with the System Developer/Maintainer review the security artifacts and make any necessary modifications
- Ensure that the System Developer/Maintainer completes the necessary CMS "Framework" phases and tasks and the system is ready for the ST&E process
- Update the overall project plan with C&A proposed schedule and key milestones
- Fully characterize the business process and the system environment in the IS RA and SSP including interconnections and information sharing
- Determine the system security level for the system
- Identify potential threats, vulnerabilities, and business risks in the IS RA
- Identify appropriate information system controls as defined by CMS policies and standards in the SSP and implement accordingly, e.g., *CMS Information Security Acceptable Risk Safeguards*
- Determine residual risk to CMS business, operations and assets in the IS RA and SSP
- Prepare other required security artifacts such as the Contingency Plan (CP)

TASK 3: ST&E RESOURCE IDENTIFICATION

The objective of this task is to notify the specific resources required to conduct the ST&E.

The Business Owner shall ensure that the following activities take place during this task:

- Determine the means for performing an independent ST&E by either:
    - Acquiring an independent C&A evaluator i.e., evaluator that has not served in a prior capacity of developing, reviewing and approving the system requirements for system under review, for the independent ST&E or
    - Contacting the Division of Resource and Acquisitions Management, Enterprise Architecture and Strategy Group, OIS for possible funding for contracting options to obtain an independent C&A evaluator and provide the funding for the independent ST&E

The C&A Evaluator shall utilize the *CMS Information Security Testing Approach* and the *CMS Information Security Reporting Standards* to perform the ST&E:

- Determine the actual level of effort to perform the ST&E
- Identify specific resources needed for the ST&E effort
- Prepare a detailed work and test plan for the ST&E activities

TASK 4: IS ARTIFACTS ANALYSIS, UPDATE, AND ACCEPTANCE

The objective of this task is to update the IS artifacts, as needed, based on the independent review by the C&A Evaluator. The completion of this task concludes the Initiation Phase of the C&A Program.

The following activities shall take place during this task:

- The C&A Evaluator shall:
    - Analyze the documented system security categorization against the *CMS System Security Level* and determine if the system has been appropriately categorized, and if

need be, advise the Business Owner of any recommended changes along with the supporting rational
    - Analyze the IS artifacts, particularly the IS RA and SSP, to determine if the internal system controls are adequate, making recommendations to the Business Owner for any changes to the information system and related IS artifacts
- The Business Owner shall update internal system controls and related security artifacts based upon the results of the independent analysis and recommendations issued by the C&A Evaluator.

3.3. PHASE 3 - SECURITY CERTIFICATION

Using independent testing, this phase determines the extent to which the internal controls in a CMS information system are implemented as described, operating with minimal risk, and producing the desired outcome. In addition, this phase addresses specific actions taken or those planned to correct deficiencies in CMS' internal system controls.

TASK 5: SECURITY CONTROL ASSESSMENT
The objective of this task is to conduct an independent assessment of the system's internal controls, i.e., ST&E. The ST&E may involve validation of IS artifacts initiated in Phase 2.

The following activities should take place during this task:

- The Business Owner shall:
    - Notify the appropriate individuals, as identified by the C&A Evaluator, to participate in the ST&E
    - Assemble all findings, results, evidence, and documentation e.g. IS RAs, annual security testing, audits, vulnerability tests, prior ST&E's, etc.
- Prior to conducting the ST&E, the Business Owner, System Developer/Maintainer, ISSO/SSO and C&A Evaluator must agree to:
    - The terms of the ST&E Rules of Engagement (RoE)
    - The ST&E procedures and evaluation techniques
- The C&A Evaluator shall utilize the *CMS Information Security Testing Approach*:
    - Develop a set of pre-requisites necessary to perform the independent ST&E and complete the C&A review
    - Review information provided by the Business Owner to determine if any previous assessment results are suitable for reuse in the current certification evaluation
    - Develop the ST&E Rules of Engagement (RoE) that will govern the testing and evaluation activities. The RoE shall address, at a minimum, the technical testing limitations, testing boundaries, administrative requirements, and procedures. The ST&E RoE shall include:
        - All of the standard RoE, unless the standard rules are unreasonable or inappropriate under the circumstances
        - System or site-specific RoE
    - Develop the ST&E Test Plan including all testing and evaluation procedures and techniques necessary to evaluate the internal controls implemented to protect the system

- Conduct the ST&E using the testing and evaluation techniques and procedures contained in the ST&E Test Plan
- Upon completion of the onsite and offsite testing, develop the ST&E Report using the *CMS Information Security Reporting Standards*

  NOTE: The completed ST&E Test Script must be annotated with the actual results and be attached to the ST&E Report.

TASK 6: SECURITY CERTIFICATION DOCUMENTATION
The objective of this task is for the Business Owner to certify the information system.

The following activities shall take place during this task:

- The C&A Evaluator shall:
  - Provide the ST&E report to the Business Owner
  - If satisfactory evidence is provided, update the status section of each corrected finding in the ST&E report prior to final issuance

- The System Developer/Maintainer shall:
  - Review and comment on the ST&E Report, and either concur with the report, refute specific vulnerability findings, or request changes to the technical content
  - Implement as many recommendations as possible before the ST&E Report is finalized to reduce or eliminate vulnerabilities and finalizing for accreditation the associated security artifacts
  - If any corrective actions are taken, notify the C&A Evaluator and provide documented / electronic evidence of the corrective actions before the final ST&E report is issued
  - Assists the Business Owner in the creation of Certification forms i.e., Certification, Certification Restrictions and Certification Actions
- The Business Owner in collaboration with the System Developer/Maintainer and the Component ISSO/SSO shall develop the CAP(s) for any remaining vulnerabilities or findings in the ST&E and document them in accordance with the *CMS Information Security POA&M Guidelines*
- The Component ISSO/SSO, the System Developer/Maintainer and Business Owner sign the Certification

3.4.PHASE 4 -SECURITY ACCREDITATION

This phase determines whether the remaining known vulnerabilities in the information system pose an acceptable level of risk to CMS business, operations, assets, and individuals. At completion of this phase, the CIO shall make one of the following three (3) decisions concerning the operation of the information system:

- Authorization to operate, i.e., Accreditation
- Conditional authorization to operate under specific terms, i.e., ATO
- Denial of authorization to operate

TASK 7: ACCREDITATION DECISION
The objective of this task is to obtain an Accreditation for the information system from the CIO.

The following activities shall take place during this task:

- The Business Owner shall:
  - Assemble and deliver the C&A package to the CISO containing at a minimum:
    - Updated IS RA
    - Updated SSP
    - Current CP
    - Latest annual CP test
    - Latest annual internal controls test (normally superseded by ST&E report)
    - ST&E report
    - Plan of Action and Milestone (POA&M) submission
    - Certification forms
    - Accreditation Letter (may be prepared by OIS)
    - Accreditation Restrictions
    - Accreditation Actions
  - Brief the CIO on the information system, its business function, its internal controls and the risk it imposes on CMS' business, operations and assets
  - Modify, if necessary, the information system and/or the C&A package based on any action items from the briefing and/or Accreditation actions
- The CISO and OIS-EASG shall:
  - Review the residual risk to CMS business, operations and assets based upon the confirmed vulnerabilities in the information system, and any planned or completed corrective actions to reduce or eliminate those vulnerabilities as stated in the C&A package prepared by the Business Owner
  - Determine if the residual risk to CMS business, operations and assets is acceptable
  - Provide concerns to the CIO, e.g., adding as accreditation actions or restrictions.
- The CIO shall:
  - Review the C&A package and consider issues discussed at the information system briefing
  - Make an accreditation decision: 1) a full Accreditation, 2) a conditional authority to operate with terms and conditions for system operation, or 3) denial to operate until required corrective actions are taken
  - Sign the IS Accreditation Letter and IS Accreditation Form, or Authority to Operate

TASK 8: C&A PACKAGE DISTRIBUTION
The objective of this task is to transmit the final C&A package to the appropriate individuals and organizations.

The completion of this task concludes the Security Accreditation Phase of the security C&A Program. The following activities shall take place during this task:

The OIS-EASG shall:

- Retain a copy of the signed C&A package

- Deliver the signed C&A package to the Business Owner

NOTE: Due to the sensitive nature of the C&A package, the Business Owner is responsible for ensuring that both the electronic and hard copies are protected according to CMS IS policy and standards.

3.5.PHASE 5 - MAINTENANCE

The Maintenance Phase provides on-going oversight, monitoring of the controls implemented specific to an information system and documentation of the status. Three basic activities happen during this phase: Continuous Monitoring, Documentation and Status Reporting, and Re-Accreditation Triggering.

TASK 9: CONTINUOUS MONITORING
The following activities shall take place for ***Configuration Management and Change Control***:

- The Business Owner shall:
  - Document proposed or actual changes to the information system
  - Performing an IS RA prior to implementing any significant changes to the system, to determine the potential business and technical impact of such changes
  - Authorize all changes to the information system
  - Develop CAPs in collaboration with the System Developer/Maintainer, when new vulnerabilities are identified and include them in the next quarterly POA&M update
- The Business Owner shall review the revised IS RA and the CAP(s) to determine if the changes increase the system risk to an unacceptable level. If the system risk level remains acceptable, the changes may proceed. If the system risk level is unacceptable, the Business Owner submits a revised C&A package for re-accreditation by the CIO. The CISO may be consulted in this determination

The following activities shall take place for ***Annual Security Control Testing***:
The Business Owner shall:

- Direct the System Developer/Maintainer and the Component ISSO/SSO to identify a sub-set of internal controls to test annually with the objective to validate all of the controls at least once every three (3) years using standard testing procedures and techniques
- Ensure the testing is conducted.
- Submit CAPs for any findings in their quarterly POA&M update.

NOTE: The *CMS Information Security Acceptable Risk Safeguards* (ARS) establishes the minimum IS standards (i.e., internal controls) for implementation in a system, as well as the basis for evaluation and validation. Annual security control testing consists of one or a combination of: performing security reviews, ST&E, vulnerability testing, CMS management directed audits, and any continuous monitoring such as intrusion detection. The Business Owner can meet the 3-year ST&E requirement (see task 5) by: 1) using an independent evaluator for annual testing and 2) by ensuring annual tests cover all internal controls within a 3-year period.

TASK 10: DOCUMENTATION AND STATUS REPORTING

The following activities shall take place:

The Business Owner shall:
- Update the IS artifacts based upon any implemented changes to the information system or changes as a result of any findings
- Provide C&A metrics and updates to the POA&M as directed by OIS-EASG

TASK 11: RE-ACCREDITATION TRIGGERING
The objective of re-accreditation is to ensure that CMS information systems continue to operate at an acceptable level of risk throughout the system's lifecycle.

The following activities shall take place during this task:

The Business Owner shall:
- Re-execute tasks 2-8 for re-accreditation (see task 9 NOTE for optional ST&E approach)
- Submit the C&A package to the CISO at least 90 days prior to the expiration of the current accreditation

+: The CIO may declare the operation of the system as unauthorized if the Business Owner does not obtain re-accreditation by the expiration of the previous accreditation.

3.6.PHASE 6 - DISPOSITION

The Disposition Phase is implemented when the system is formally retired and ceases to exist as an operational system. This phase ends the SDLC process. Disposition of the automated system occurs based on the System Disposition Plan to ensure that all confidential and proprietary information were properly handled.

TASK 12: DEVELOP SYSTEM DISPOSITION PLAN
The objective of this task is develop a System Disposition Plan that addresses how the various components of the automated system (software, data, hardware, communications, and documentation) are to be handled at the completion of operations to ensure proper disposition of all the system components and to avoid disruption of the individuals and / or other systems impacted by the disposition.

The following activities should take place during this task:

The Business Owner shall:
- Develop a System Disposition Plan
- Verify that software/applications have not been compromised
- Archive or transfer data, software components and life cycle documentation and artifacts

TASK 13: DISPOSE OF EQUIPMENT
The following activities should take place during this task:

The Business Owner shall:

- Ensure that equipment is disposed off in accordance with the System Disposition Plan. Any equipment that can be used elsewhere in the organization shall be recycled.

TASK 14: CONDUCT A DISPOSITION REVIEW
The objective of this task is to conduct a review to ensure that a system/application or other IT situation has been completely and appropriately disposed, thereby ending the lifecycle of the IT investment.

The following activities should take place during this task:
The Business Owner shall:

- Conduct a disposition review
- Document the lessons learned from the shutdown and archiving of the terminated system.

APPENDIX A C&A ACTIVITIES CHECKLIST

System Name	
Business Owner	

STEPS	DATE COMPLETED	COMPLETED BY
PHASE 1: PRE-CERTIFICATION		
Task 1-Business Risk Identification		
1. Include C&A resources in IT investment request		
2. Initiate IS RA development		
3. Identify business risk		
PHASE 2: INITIATION		
Task 2-Certification Preparation		
1. Prepare C&A project plan indicating proposed schedule, resources and key milestones		
2. Continue IS RA development		
3. Initiate SSP development		
4. Fully characterize the system in the SSP		
5. Identify system security level		
6. Identify risks in the IS RA		
7. Identify controls in the SSP		
8. Evaluate residual risks		
9. Prepare IS artifacts		
Task 3-ST&E Resource Identification		
1. Determine ST&E required resources 2. Notify ST&E participants		
Task 4-IS Artifacts Analysis, Update and Acceptance		
1. Independent review of the Security Categorization (System Security Level)		
2. An independent analysis of the IS artifacts, e.g., IS RA, SSP, CP etc.		
3. Update IS artifacts as needed		
PHASE 3: SECURITY CERTIFICATION		
Task 5-Security Control Assessment		
1. Prepare for the assessment		
2. Negotiate the RoE		
3. Conduct the assessment		
4. Document the results		
Task 6-Security Certification Documentation		
1. Provide the ST&E findings and certification recommendations to the Business Owner		
2. Update the IS artifacts as needed		
3. Prepare the POA&M based on the ST&E findings		

STEPS	DATE COMPLETED	COMPLETED BY
4. Prepare the Business Owner Certification		
PHASE 4: SECURITY ACCREDITATION		
Task 7-Accreditation Decision		
1. Assemble the C&A package		
2. Determine if the agency-level risk is acceptable		
3. Prepare accreditation recommendations		
4. Submit C&A package to CIO		
5. Business Owner C&A briefing to CIO		
6. Sign Accreditation Letter or ATO		
Task 8-C&A Package Distribution		
1. Distribute the C&A package to the Business Owner		
2. Update the SSP with the latest information from the accreditation decision		
PHASE 5: MAINTENANCE		
Task 9-Continuous Monitoring		
Configuration Management and Change Control		
1. Authorize and 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		
3. Submit CAPs in quarterly POA&M		
Security Control Testing		
1. Select an appropriate set of security controls to be tested		
2. Annually assess the selected controls using standard procedures and techniques		
Task 10-Documentation and Status Reporting		
1. Update the IS artifacts		
2. Update the POA&M		
3. Report the C&A metrics to the CISO		
Task 11-Re-Accreditation Triggering		
1. Re-execute tasks 2-8		
2. Submit C&A Package		
PHASE 6: DISPOSITION		
Task 12-Develop System Disposition Plan		
1. Develop a System Disposition Plan		
2. Verify that software/applications have not been compromised		
3. Archive or transfer data, software components, life cycle documents and artifacts		
Task 13-Dispose of Equipment		
1. Ensure that equipment is disposed of in accordance with the System Disposition Plan		

STEPS	DATE COMPLETED	COMPLETED BY
Task 14-Conduct a Disposition Review		
1. Conduct a disposition review		
2. Document the lessons learned from the shutdown and archiving of the terminated system		

APPENDIX B ACRONYMS

ARS	Acceptable Risk Safeguards
ATO	Authority to Operate (conditional)
C&A	Certification & Accreditation
CAP	Corrective Action Plans
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
CP	Contingency Plan
DAA	Designated Approving Authority
EASG	Enterprise Architecture & Strategy Group
FISMA	Federal Information Security Management Act
GSS	General Support System
IS	Information Security
IS RA	Information System Risk Assessment
ISSO	Information System Security Officer
MA	Major Application
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestone
OIS	Office of Information Services
RA	Risk Assessment
RoE	Rules of Engagement
SDLC	System Development Life Cycle
SSO	System Security Officer
SSP	System Security Plan
ST&E	Security Test & Evaluation

End of Document