# Contents

# Exhibits

This page intentionally left blank

# 1 Introduction

## 1-1 About This Handbook

This handbook does the following:

a. Contains a description of the Postal Service™ information resource certification and accreditation (C&A) process.

b. Identifies the roles and responsibilities in the process.

c. Provides pointers to instructions and templates to complete each phase of the process.

Certification is the technical analysis that establishes the extent to which an information resource meets specified security requirements. Accreditation is the management analysis that determines, from a business standpoint, whether implemented security controls satisfy specified security requirements and provide an acceptable level of risk.

The information resource C&A process is integrated in the information technology (IT) technical solution life cycle (TSLC).

## 1-2 Purpose of Certification and Accreditation

The C&A is the process the Postal Service uses to evaluate the protection of its information resources so that risks associated with deployment can be appropriately managed throughout the life cycle.

## 1-3 Importance of Certification and Accreditation

The C&A process provides Postal Service business owners with a consistent method for making informed decisions on managing security risks related to their information resources. Benefits include the following:

a. A structured view of the potential risks associated with information resources and the relationships among business partnerships.

b. Determination of sensitivity which is the degree to which the Postal Service must protect the confidentiality and integrity of information. Levels of sensitivity are sensitive-enhanced, sensitive, and nonsensitive.

c. Determination of criticality which is the degree to which the Postal Service must provide for continuous availability of information and the

protection of the health and safety of personnel. Levels of criticality are critical and noncritical.

d. Documentation of the information security controls and processes needed to protect the confidentiality, integrity, and availability of Postal Service information resources.

e. Systematic approach to the initial and periodic test of those controls and processes.

f. The development of standard operating procedures and training.

g. Protection of the privacy of employees and customers. Privacy is the protection afforded individuals and customers from the collection, storage, and dissemination of information about themselves and possible compromises resulting from unauthorized release of that information.

h. Protection of Postal Service assets and brand.

i. Compliance with the intent of applicable federal laws and regulations.

# 2 Roles and Responsibilities

This chapter defines the roles and responsibilities for the information resource C&A process. (See Exhibit 2, Relationship of C&A Roles.)

## 2-1 Chief Inspector

The chief inspector is responsible for the following:

a. With information systems security officers, conducting site security reviews of facilities containing Postal Service computer and telecommunications equipment to evaluate all aspects of physical, environmental, and personnel security.

b. Providing technical guidance on physical and environmental security activities that support information security, such as controlled areas, access lists, physical access control systems, and identification badges; providing protection of workstations, portable devices, and media containing sensitive-enhanced, sensitive, or critical information.

c. Providing security consultation and guidance during system, application, and product development to assure that security concerns are addressed and information and/or evidence that may be needed for an investigation is retained by the information resource.

d. Investigating reported security violations and conducting revenue/financial investigations including theft, embezzlement, or fraudulent activity.

e. Providing physical protection and containment assistance and investigating information security incidents as appropriate.

## 2-2 Executive Vice President, Chief Information Officer

The executive vice president (VP), chief information officer (CIO), is responsible for the following:

a. Acting as the senior IT decision maker and corporate change agent to securely integrate the key components of business transformation: technology, processes, and people.

b. Providing advice and assistance to senior managers on information security policy and their compliance-based performance.

c. Promoting the implementation of an information security architecture to mitigate information security-related risk.

d. Promoting the protection of corporate information resources across Postal Service organizations and business partners.

## 2-3 Vice President, Information Technology

The VP, IT, is responsibile for the following:

a. Sponsoring information security and business continuity management programs and ensuring that financial, personnel, and physical resources are available for completing security and business continuity tasks.

b. Ensuring confidentiality, availability, and integrity of information processed by IT applications.

c. Ensuring compliance with the information security certification and accreditation processes.

d. Accepting all risks, liabilities, and responsibilities and assuming personal accountability for any damage to the Postal Service (including direct financial losses and any costs resulting from remedial actions in operating the information resource) for authorizing an information resource to enter the production environment prior to completing the information resource C&A process.

e. Together with the vice president of the functional business area, accepting, in writing, residual risk of applications and approving their deployment or continued deployment. The VP IT may delegate this responsibility to the applicable portfolio manager. If this responsibility is delegated, notice to that effect must be in writing.

f. Defining and documenting secure coding best practices.

## 2-4 Manager, Computer Operations

The manager, Computer Operations, is responsible for the following:

a. Sponsoring information security and business continuity management programs and ensuring that financial, personnel, and physical resources are available for completing security and business continuity tasks.

b. Ensuring confidentiality, availability, and integrity of information processed at IT sites.

c. Ensuring the protection and secure implementation of the Postal Service IT infrastructure.

d. Supporting the information security certification and accreditation processes.

e. Reviewing and utilizing C&A documentation in the IT Artifacts Library.

## 2-5 Manager, Corporate Information Security Office

The manager, Corporate Information Security Office (CISO), is responsible for the following:

a. Developing, guiding, and maintaining the C&A process.

b. Managing the CISO support for the C&A process.

c. Appointing information systems security officers (ISSOs) and the certifier (program manager security C&A process).

d. Reviewing the C&A documentation package and accrediting the information resource.

## 2-6 Vice Presidents of Functional Business Areas

Vice presidents of functional business areas are responsible for the following:

a. Funding information security throughout the life cycle of information resources under their purview.

b. Together with the VP IT, accepting, in writing, residual risks associated with applications under their control and approving their deployment or continued deployment. The vice president of the functional business area may delegate this responsibility to the applicable executive sponsor. If this responsibility is delegated, notice to that effect must be in writing.

## 2-7 Executive Sponsors

The executive sponsors, as representatives of the VPs of the functional business areas, are responsible for ensuring the completion of all security-related tasks throughout the life cycle of an information resource. Some information resources are developed under the direction of one executive sponsor in one organization and transferred to an executive sponsor in another organization for production. Executive sponsors are responsible for the following:

a. Completing a business impact assessment (BIA) to determine the sensitivity and criticality of information resources under their purview.

b. Funding the C&A process for information resources under their purview.

c. Appointing, if desired, an information systems security representative (ISSR) to serve as a development team point of contact to perform security-related activities.

d. Implementing security controls that satisfy the security requirements defined in the BIA.

e. Ensuring that all documentation required by the C&A process is submitted to the ISSO.

f. Maintaining appropriate security during the production phase by controlling access to sensitive-enhanced, sensitive, and critical information.

g. Ensuring that the C&A documentation package is securely stored and kept current for the information resource life cycle.

h. If the vice president functional business area delegated this responsibility to the executive sponsor, the executive sponsor will work jointly with the VP IT (or the portfolio manager if this responsibility is delegated) to review the C&A documentation package, accept the residual risk to an application, and approve the application for production or return the application to the applicable life cycle phase for rework.

i. Re-initiating the C&A process in accordance with the criteria specified in Chapter 6.

## 2-8 Portfolio Managers

Portfolio managers are responsible for the following:

a. Functioning as the liaison between executive sponsors and the information technology providers.

b. Ensuring that the information resource is entered in the Enterprise Information Repository (EIR) and the record is updated as required.

c. Appointing, if desired, an ISSR to serve as a development team point of contact to perform security-related activities.

d. Reviewing the C&A documentation package and completing a risk mitigation plan for risks identified as High or Medium.

e. Preparing and signing an acceptance of responsibility letter, if a documented High or Medium vulnerability will not be mitigated.

f. Ensuring that the information resource is registered in eAccess and updated as required.

g. Ensuring C&A documentation is stored in the IT Artifacts Library and maintaining the hardcopies and electronic copies for the appropriate retention periods.

h. Maintaining appropriate security during the production phase by ensuring the installation of software and operating system security patches.

i. If the VP IT delegated this responsibility to the portfolio manager, the portfolio manager will work jointly with the vice president of the functional business area (or the executive sponsor if this responsibility is delegated) to review the C&A documentation package, accept the residual risk to an information resource, and approve the information resource for production or return the information resource to the applicable life cycle phase for rework.

## 2-9 Project Managers

Project managers for application development, acquisition, or integration projects are responsible for the following:

a. Managing day-to-day development and implementation efforts for new information resources, whether developed in-house, outsourced, or acquired.

b. Incorporating the appropriate security controls in all information resources, whether developed in-house, outsourced, or acquired, to satisfy the security requirements defined in the BIA.

c. Entering the information resource in the EIR and updating the record as required.

d. Storing C&A documentation in the IT Artifacts Library and retaining hardcopies and electronic copies for the appropriate retention periods.

e. Assuming the role of the ISSR if one is not appointed.

## 2-10 Chief Privacy Officer

The chief privacy officer (CPO) is responsible for the following:

a. Ensuring compliance with privacy requirements.

b. Developing policy related to defining information sensitivity.

c. Consulting with the executive sponsor on determining information sensitivity designations during the completion of the BIA and all equivalent stages of the BIA re-certification procedure; reviewing the BIA after completion; and approving the determination of information sensitivity.

d. Developing appropriate data record retention, disposal, and release guidelines.

## 2-11 Certifier

The program manager, security C&A process, who is appointed by the manager, CISO, functions as the certifier. The certifier is responsible for the following:

a. Reviewing the C&A evaluation report and the supporting C&A documentation package.

b. Escalating security concerns or preparing and signing a certification letter.

c. Forwarding the certification letter and C&A documentation package to the portfolio manager.

## 2-12 Accreditor

The manager, CISO, functions as the accreditor and is responsible for the following:

a. Reviewing the risk mitigation plan and supporting C&A documentation package together with business requirements and relevant Postal Service issues.

b. Escalating security concerns or preparing and signing an accreditation letter that makes one of the following recommendations: accepting the information resource with its existing information security controls, requiring additional security controls with a timeline to implement, or deferring deployment until information security requirements can be met.

c. Forwarding the accreditation letter and C&A documentation package to the portfolio manager and executive sponsor.

## 2-13 Information Systems Security Officers

ISSOs are responsible for the following:

a. Providing information security and C&A guidance.

b. Facilitating initial briefings and subsequent meetings of the C&A core team.

c. Coordinating the completion of a BIA for each information resource.

d. Providing advice and consulting support to executive sponsors and portfolio managers during the BIA process regarding the baseline security requirements that apply to all information resources (including nonsensitive and noncritical) and the additional security requirements required to protect sensitive-enhanced, sensitive, and critical information resources.

e. Working with the Privacy Office on privacy-related requirements.

f. Recommending security requirements to executive sponsors and portfolio managers during the BIA process based on generally accepted industry practices, the operating environment [e.g., hosted in the de-militarized zone (DMZ)], and the risks associated with the information resource.

g. Providing guidance on how information resources are vulnerable to threats, what controls and countermeasures may be appropriate, and the C&A process.

h. Reviewing and evaluating C&A documentation, including the BIA, risk assessment, security plan, security test and evaluation (ST&E) plan and report, and independent reviews of the information resource.

i. Preparing and signing the C&A evaluation report.

j. Escalating security concerns or forwarding the C&A evaluation report and supporting C&A documentation package to the certifier.

k. Working jointly with the Inspection Service, conducting site security reviews.

## 2-14 Information Systems Security Representatives

The information systems security representative (ISSR) may be appointed by an executive sponsor or portfolio manager to serve as a development point of contact to perform security-related activities on their behalf. The ISSR role is an ad hoc responsibility performed in conjunction with other assigned duties. If an ISSR is not appointed, the project manager assumes the ISSR responsibilities. ISSR responsibilities include the following:

a. Providing support to the executive sponsor and portfolio manager, as required.

b. Promoting information security awareness on the project team.

c. Ensuring that security controls and processes are implemented.

d. Notifying the executive sponsor, portfolio manager, and ISSO of any additional security risks or concerns that emerge during development, acquisition, or integration of the information resource.

e. Developing security-related documents required by the C&A process.

f. Working with the ISSO to complete C&A artifacts and sending the other required artifacts (e.g., TAD and security specifications for procurements) to the ISSO.

## 2-15 Contracting Officers

Contracting officers, and employees approving non-Supply Management contracts, are responsible for the following:

a. Ensuring that information technology contractors, vendors, and business partners are contractually obligated to abide by Postal Service information security policies, requirements, standards, and procedures, including the C&A process.

b. Ensuring that all contracts and business agreements requiring access to Postal Service information resources identify sensitive positions, specify the clearance levels required for the work, and address appropriate security requirements.

c. Ensuring that contracts and business agreements allow monitoring and auditing of any information resource project.

d. Ensuring that the security provisions of the contract and business agreements are met.

e. Confirming the employment status and clearance of all contractors who request access to information resources.

f. Ensuring all account references, building access, and other privileges are removed for contractor personnel when they are transferred or terminated.

## 2-16 Business Partners

Business partners developing or hosting information resource for the Postal Service are responsible for the following:

a. Abiding by Postal Service information security policies, regardless of where the information resources are located or who operates them.

b. Implementing and maintaining security controls to meet assurance level and contractual security requirements.

c. Making necessary changes to security controls to reduce risk to an acceptable level as defined by Postal Service representatives.

d. Implementing and complying with privacy requirements.

## 2-17 Disaster Recovery Services

Disaster Recovery Services (DRS) is responsible for the following:

a. Providing consulting support to executive sponsors and portfolio managers regarding disaster recovery planning.

b. Reviewing the contingency planning documents and accepting them as complete or returning it to the executive sponsor for rework.

c. Storing the accepted contingency planning documents.

d. Supporting the exercise of contingency plans.

## 2-18 Functional System Coordinators

A functional system coordinator (FSC) is a customer representative assigned to an information resource who is responsible for the following:

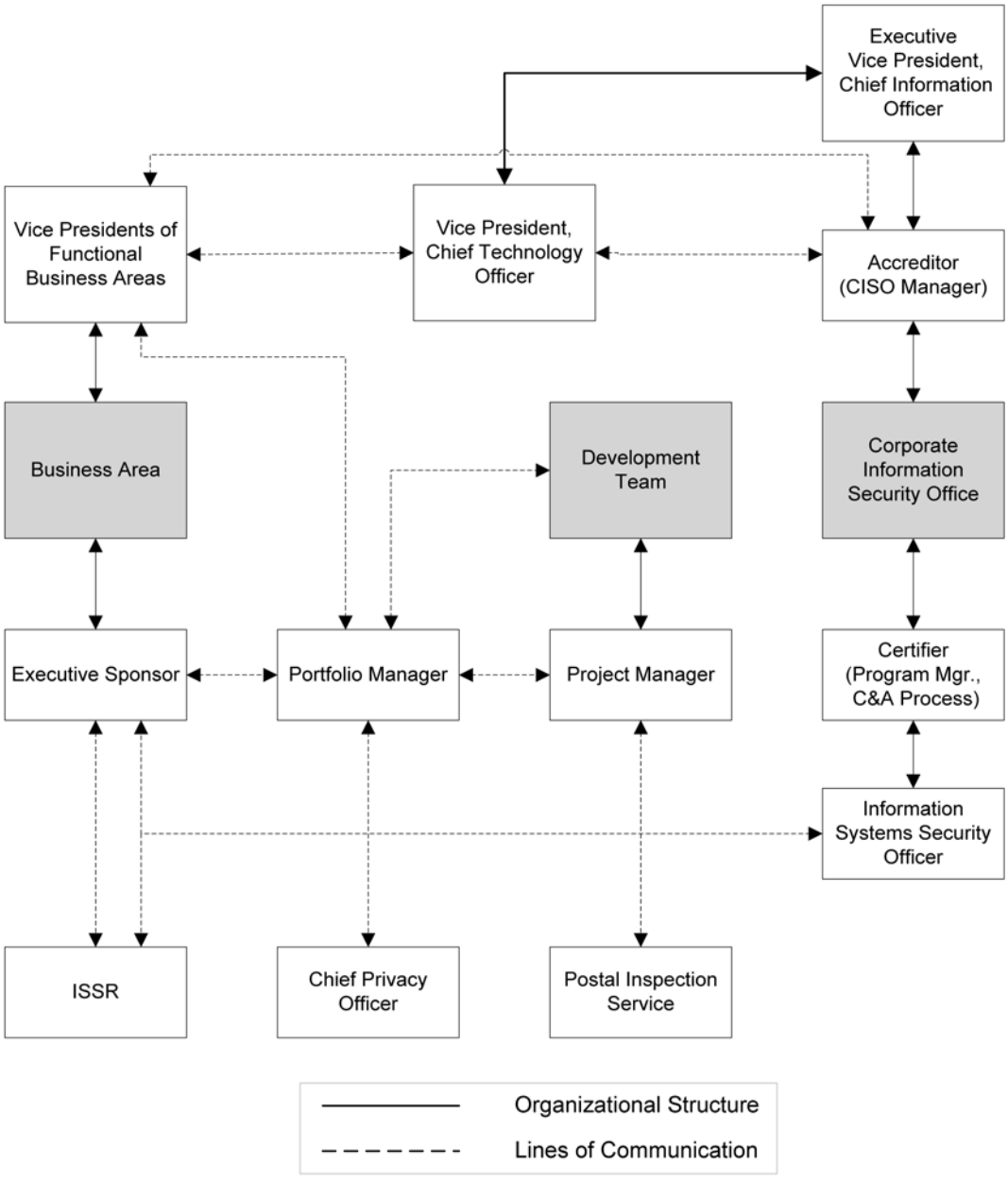
a. Approving access to the information resource after the requestor's manager has approved the request.

b. Participating in the eAccess generated semi-annual review to ensure each user/role is correct from a business point of view.

## 2-19 Functional System Gatekeepers

A functional system gatekeeper (FSG) is designated by the information resource owner to approve the FSCs for a given information resource. eAccess will e-mail the FSG in the event all FSCs are no longer active for a given information resource.

Exhibit 2
**Relationship of Certification and Accreditation Roles**



This page intentionally left blank

# 3 Information Designation and Control

## 3-1 Elements of the Certification and Accreditation Process

The C&A process consists of the following seven interrelated phases that are conducted concurrently with the development and deployment of new information resources (see Exhibit 3-1):

a. Phase 1 — Initiate and Plan.
b. Phase 2 — Requirements.
c. Phase 3 — Analysis and Design.
d. Phase 4 — Build.
e. Phase 5 — System Integration Testing (SIT).
f. Phase 6 — Customer Acceptance Testing (CAT).
g. Phase 7 — Release and Production.

The C&A process does the following:

a. Determines the sensitivity and criticality of Postal Service information resources.
b. Defines information security requirements.
c. Determines appropriate security controls and processes to satisfy the security requirements.
d. Tests the effectiveness of implemented security controls and processes.
e. Evaluates the threats and vulnerabilities associated with the information resources and the risks associated with deployment.
f. Culminates with certification, risk acceptance, accreditation, and approval to deploy the information resource.

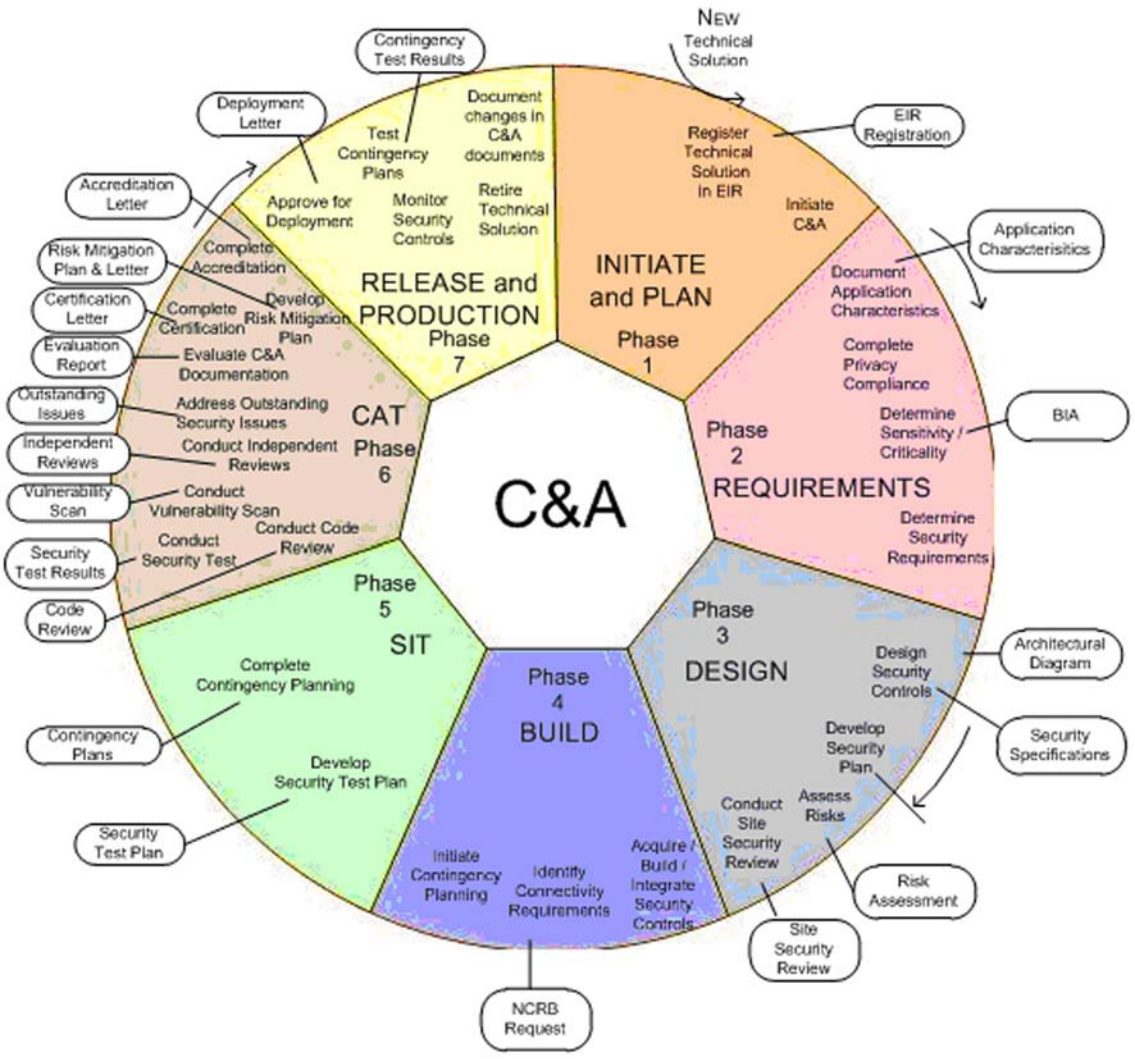
During the release and production phase, the C&A process ensures the information resource is maintained with the appropriate security, residual risk is appropriately managed, and when the information resource is retired equipment is sanitized and sensitive-enhanced and sensitive information is appropriately destroyed.

# 3-2 What the Certification and Accreditation Process Applies To

The C&A process applies to all information resources (new, small, or field) sponsored by, developed for, or maintained or operated on behalf of the Postal Service, whether or not they are located at a Postal Service facility. The C&A also applies to pilot and proof-of-concept projects.

Consult with the CISO as soon as an information resource is conceived.

Exhibit 3-1
**Certification and Accreditation Phases and Major Deliverables**




## 3-2.1 Typical Information Resources

Exhibit 3-1 depicts the seven TSLC phases and the major activities and deliverables required during each phase for typical information resources.

### 3-2.2 Small Information Resources

If the information resource is small, it may be suitable for a rapid security review process. Small information resources generally are those that:

a. Are hosted by IT.

b. Face internally.

c. Contain few Web pages.

d. Have a limited number of interfaces.

e. Have a limited amount of code.

f. If using a commercial off-the-shelf (COTS) product, the product is on the Infrastructure Toolkit.

***Note:*** The rapid review process generally does not apply to information resources that are designated as sensitive-enhanced or sensitive; or to business, financial, or publicly facing (i.e., Internet accessible) information resources. However, exceptions may occur based on guidance from the CIO or the VP IT Solutions.

### 3-2.3 Field Information Resources

Field information resources are not national information resources and are hosted on a server located in the Field Information Systems Server Farm at Eagan, MN. Field information resources are designated as noncritical and can never be critical. Field information resources facilitate the completion of one or more specific tasks, establish a unique session with each user, and allow users to make permanent changes to stored data.

## 3-3 Frequency of Certification and Accreditation

Re-initiating the information resource C&A process is required every year for payment card industry information resources and every 3 years for sensitive-enhanced, sensitive, and critical information resources, and every 5 years for all other information resources.

Re-initiating the C&A could also be required if the information resource undergoes a significant change, a significant information security incident, a significant audit finding, or at the request of the CIO, VP IT Solutions, CISO, the VP of the function business area, or the executive sponsor. A significant change is a change that calls into question the security of an information resource and the accuracy of previous C&A documentation. See Chapter 6, Re-Initiating the C&A, for specific examples.

## 3-4 Funding

Funding for the C&A process should be determined before development efforts begin and included as part of the overall development project funding. The scope and funding should be discussed with business partners and

contractors before development begins especially when the business partners must conduct some of the tasks associated with the C&A process.

## 3-5 Certification and Accreditation Core Team

The core team consists of those personnel who are actively involved in and responsible for completing the documentation and activities in the C&A and includes the following personnel or their representatives:

a. Executive sponsor.

b. Portfolio manager.

c. Project manager.

d. Information systems security officer.

e. Information systems security representative.

f. Disaster Recovery Services representative.

g. Privacy representative

# 4 Certification and Accreditation Process

This chapter describes each phase in the C&A process. At the end of this chapter, Exhibit 4-7b provides a list of C&A guidelines, templates, and related Web links; Exhibit 4-7c provides a summary of deliverables by phase.

## 4-1 Phase 1 — Initiate and Plan

Phase 1 applies to information resources sponsored by, developed for, or maintained or operated on behalf of the Postal Service, whether or not they are located at a Postal Service facility. It can be applied to pilot, new, and production information resources and business partner initiatives. The C&A process begins when an executive sponsor or portfolio manager sends a letter or email to the manager, CISO, requesting the initiation of the C&A process. (See Exhibit 4-1, Phase 1, Initiate and Plan.)

### 4-1.1 Objectives

The objectives for this phase are as follows:

a. Registering the information resources in the EIR.

b. Initiating the C&A process.

### 4-1.2 Deliverables

The deliverables for this phase are the following:

a. EIR registration.

b. Notification to the manager, CISO, to initiate the C&A process.

### 4-1.3 Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Executive sponsor | Ensures completion of Phase 1 activities. |
| Portfolio manager | Provides guidance and assistance. |
| Project manager | Registers information resources in EIR. |
| ISSR | Supports executive sponsor and portfolio manager as requested. |
| ISSO | Facilitates meetings of the C&A core team. |

## 4-1.4 Activities

### 4-1.4.1 Register Information Resource in Enterprise Information Repository

The project manager registers the information resources in EIR.

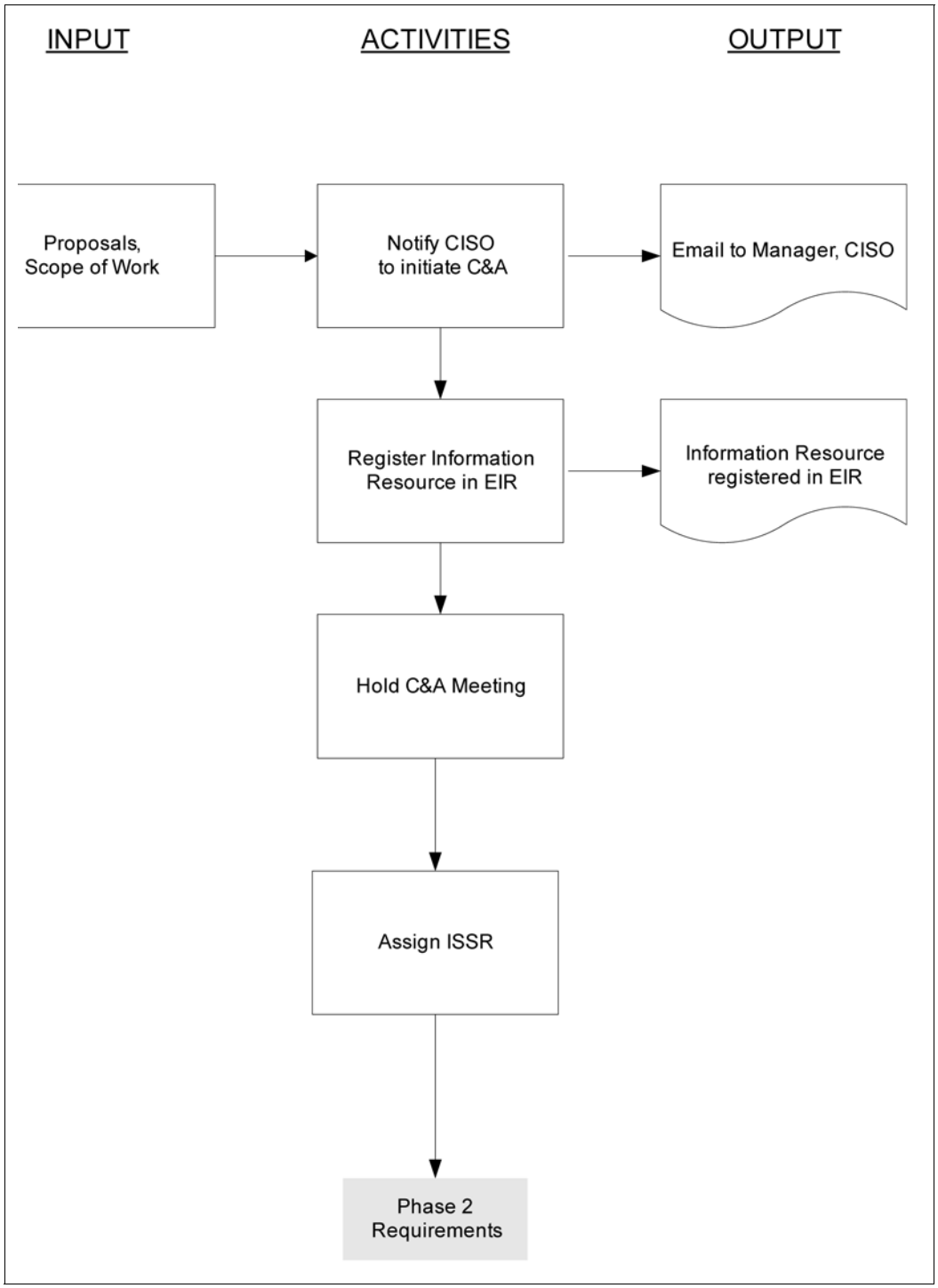
### 4-1.4.2 Hold Certification and Accreditation Meeting

The ISSO assigned to the information resources assembles the C&A core team to discuss the proposed information resources and its business requirements and review the C&A process. The ISSO is encouraged to pursue flexible and cost-effective communication approaches, such as teleconferencing or videoconferencing. The ISSO provides the project team with copies of the templates to be completed.

### 4-1.4.3 Assign Information Systems Security Representative

The executive sponsor or portfolio manager may assign, in writing, an ISSR to perform security-related activities. If an ISSR is not appointed, the project manager assumes the ISSR responsibilities.

Exhibit 4-1
**Phase 1, Initiate and Plan**



# 4-2 Phase 2 — Requirements

Phase 2 determines the requirements for the information resource or technical solution. (See Exhibit 4-2, Phase 2, Requirements.)

## 4-2.1 Objectives

The objectives for this phase are as follows:

a. Documenting application characteristics including the following:
   (1) Describing the development environment.
   (2) Describing the testing environments (both SIT and CAT).
   (3) Describing the production environment.
   (4) Describing the Non Postal Service environment.
   (5) Describing the network connectivity characteristics.
   (6) Documenting the sensitive and sensitive-enhanced data elements.
   (7) Developing a high-level architectural diagram.
   (8) Identifying application internal and external dependencies.

b. Conducting the BIA.
   (1) Ensuring privacy compliance.
   (2) Determining the sensitivity and criticality of the information resource.
   (3) Generating security requirements to mitigate risk based on sensitivity, criticality, and the business needs of the Postal Service.

c. Updating a Plan of Action and Milestones (POA&M) and EIR. The POA&M is also known as the TSLC Project Plan.

## 4-2.2 Deliverables

The deliverables for this phase are the following:

a. Application Characterization.

b. BIA.

c. Updated POA&M and EIR.

## 4-2.3 Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Executive sponsor | Ensures completion of Phase 2 activities. |
| Portfolio manager | Provides guidance and assistance. |
| ISSR | Supports executive sponsor and portfolio manager as requested. |
| ISSO | Facilitates meetings of the C&A core team.<br>Coordinates completion of BIA.<br>Provides advice and consulting support to executive sponsors and portfolio managers regarding the baseline security requirements that apply to all information resources and the additional security requirements required to protect sensitive-enhanced, sensitive, and critical information resources.<br>Coordinates with the Privacy Office on privacy-related requirements.<br>Recommends additional security requirements to executive sponsors and portfolio managers based on threats, vulnerabilities, and generally accepted industry practices. |
| Privacy Office | Reviews Privacy Impact Assessment and approves determination of sensitivity. |
| Development Team | Completes Application Characterization, BIA, updates POA&M, updates EIR, and keeps C&A core team informed of progress. |

## 4-2.4 Activities

### 4-2.4.1 Review Documentation

The C&A core team reviews documentation that they receive. Some of the documentation could include the following:

a. Original business needs statement, business case, request for proposals, statement of work, and TSLC requirements documentation.

b. Contracts and POA&M.

c. Policies, procedures, standards, and any other applicable documentation that may affect the information resource.

### 4-2.4.2 Document Application Characteristics

The Project Manager or ISSR document the application characteristics which includes the following steps:

a. Answering the development environment section questions.

b. Answering the testing environments (both SIT and CAT) section questions.

c. Answering the production environment section questions.

d. Answering the non Postal Service environment section questions.

e. Answering the network connectivity characteristics section questions.

f. Documenting the sensitive and sensitive-enhanced data elements.

g. Developing a high-level architectural diagram (i.e., physical layer 1 topology including what ports are listening on each device, firewalls, routers, switches, communication protocols and devices, security devices, and interconnected resources).

h. Identifying application internal and external dependencies to document how a given application interfaces with the rest of the Postal Service applications and infrastructure. The project manager and ISSR may need to meet with developers, system administrators, network administrators, database administrators, the portfolio manager, and customer representatives to complete the internal and external dependencies table. A system is dependent if it CANNOT function without the input or connection to the other system or portal. For example, applications which by themselves are not critical may have a higher designation because they provide data to an application with a higher criticality designation.

### 4-2.4.3 Conduct Business Impact Assessment

The ISSO coordinates the completion of the BIA, which includes the following steps:

a. Completing the privacy section.

b. Determining sensitivity (i.e., sensitive-enhanced, sensitive, or nonsensitive).

c. Determining criticality, (i.e., critical-high, critical-moderate, or noncritical [low]).

d. Determining security requirements. Security requirements are defined for all information resources to secure the information resources commensurate with the risk. Security requirements include:

(1) Baseline security requirements for all information resources.

(2) Additional security requirements based upon the sensitivity and criticality of the information resource and industry requirements.

(3) Additional conditional requirements based on request by senior management or specific criteria.

(4) Additional security requirements recommended by the ISSO based on generally accepted industry practices, the operating environment, and the risks associated with the information resource.

e. Signing Acceptance of Responsibility and Verification sections of BIA. (The portfolio manager or their designee, the executive sponsor or their designee, privacy official, and ISSO sign these sections relevant to their function.)

***Note:*** Some information resources are developed under the direction of one executive sponsor in one organization and transferred to an executive sponsor in another organization for Phase 7 of the C&A process (Release and Production).

Template and instructions for completing the BIA are available on the Information Technology Web site. Select TSLC Templates; under the Requirements phase, select BIA Security Requirements.

### 4-2.4.4 Update Plan of Action and Milestones and Enterprise Information Repository

Once the BIA is completed, the portfolio manager ensures that the EIR is updated and amends the POA&M to include integrating information security controls in the information resource and the deliverables associated with the C&A process.

The POA&M, a key document in the security certification and accreditation package, describes actions taken or planned by the executive sponsor to correct deficiencies in the security controls and to address remaining vulnerabilities in the information resource. The POA&M identifies:

a. Tasks needing to be accomplished to address vulnerabilities.

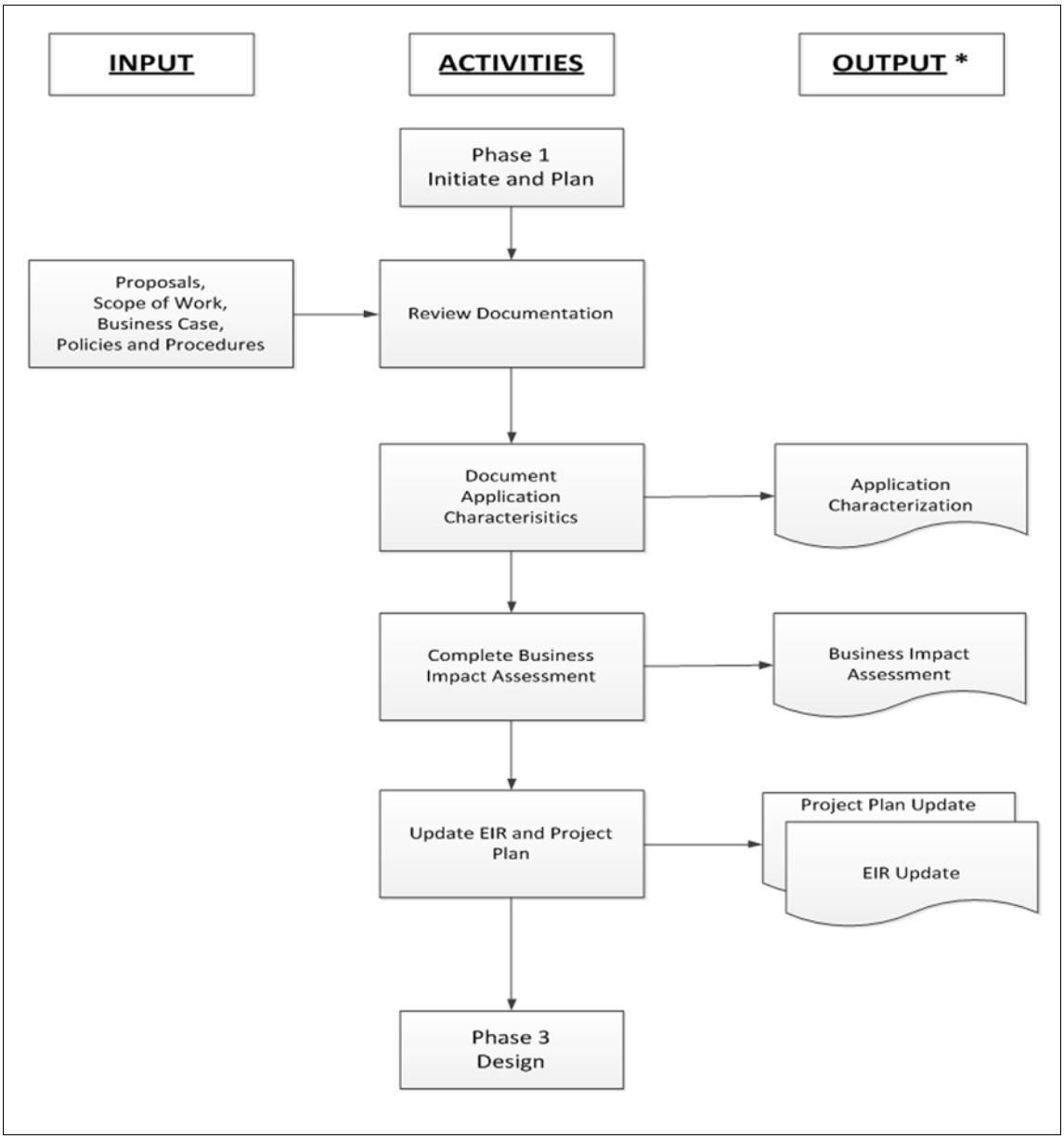
b. Resources required to accomplish the elements in the plan.

c. Milestones in meeting the plan.

d. Scheduled completion dates for the milestones.

The POA&M is updated throughout the information resource lifecycle for changes to the hardware, software, firmware, and the surrounding computing environment.

Exhibit 4-2
**Phase 2, Requirements**



# 4-3 Phase 3 — Design

Phase 3 identifies security controls and processes for the security requirements defined in Phase 2, Requirements. (See Exhibit 4-3, Phase 3, Design.)

## 4-3.1 Objectives

The objectives for this phase are as follows:

a. Documenting the security specifications.

b. Identifying security controls and processes for security requirements documented in the BIA.

c. Selecting security controls on their ability to meet security requirements and provide a cost-effective security solution.

d. Developing a security plan.

e. Conducting a risk assessment.

f. Conducting a site security review, if required.

## 4-3.2 Deliverables

The deliverables for this phase are the following:

a. Security specifications.

b. Security plan.

c. Risk assessment.

d. Site security review, if required.

## 4-3.3 Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Executive sponsor | Ensures completion of Phase 3 activities. |
| Portfolio manager | Provides guidance and assistance. |
| ISSR | Supports executive sponsor as required. |
| ISSO | Provides guidance and consulting support for completion of C&A deliverables. |
| Development Team | Prepares deliverables and keeps C&A core team informed of progress. |

## 4-3.4 Activities

### 4-3.4.1 Document Security Specifications

Security specifications are documented to satisfy the security requirements defined by the BIA. The security specifications will be included in contracts and acquisitions as appropriate.

### 4-3.4.2 Analyze Requirements and Identify Potential Security Controls

Analyze the security requirements established for the information resource and identify potential security controls in light of business requirements,

Postal Service policies, project schedule, budget, and cost versus benefit of the various control options. See the Information Security Requirements and Controls document available on the IT Web site. Select TSLC Templates; under the Analysis and Design phase, select Information Security Requirements and Controls for examples of controls and processes that can be used to fulfill the security requirements.

Security controls include countermeasures and safeguards. A countermeasure is a control against known threats where as a safeguard is a control against future unknown threats. Security controls can be characterized as preventive, detective, corrective, deterrent, compensating, continuous, management, and technical.

Security controls will be selected or designed, purchased or built, integrated, and configured to address the security requirements and bring residual risk to an acceptable level by reducing the likelihood that vulnerabilities will be exploited and/or by reducing the amount of harm that could occur if a given vulnerability is exploited.

## 4-3.4.3 Select/Design Security Controls

### 4-3.4.3.1 General

Security controls for the information resource are selected to satisfy the privacy and security requirements identified in the BIA and to mitigate the risks identified in the Risk Assessment.

Security controls include the following:

a. Management controls:
   (1) Background screening and clearances.
   (2) Job descriptions.
   (3) Performance appraisals.
   (4) Progressive sanctions.
   (5) Condition of employment.
   (6) Separation of duties and responsibilities.
   (7) Dual control of “critical” processes and keys.
   (8) Risk management.
   (9) Configuration/change management.
   (10) Independent reviews.

b. Operational controls:
   (1) Personnel security.
   (2) Media protection.
   (3) Physical protection (e.g., badges, controlled areas, visitors, and equipment and media removal).
   (4) Environmental protection.
   (5) Contingency planning.
   (6) Incident response process.
   (7) Hardware/system software maintenance.
   (8) Network connectivity review board.

(9) Operational security training.

(10) Security awareness training.

(11) Audit logging.

(12) Testing of security controls.

(13) Continuous monitoring.

c. Technical controls:

(1) Platform hardening.

(2) Identification and authentication.

(3) Logical access.

(4) Communications.

(5) Encryption

(6) Integrity checking.

(7) Vulnerability scans.

(8) Penetration testing.

(9) Hardware and media sanitization.

Multiple information security controls may be needed to satisfy a particular information security requirement, or one control may satisfy more than one information security requirement.

#### 4-3.4.3.2 Selecting Security Controls

Information security controls are selected based on their capability to be implemented, their effectiveness in safeguarding the information resource and the information processed, their compatibility with other Postal Service security controls and processes and business needs. Circumstances peculiar to the information resource, the computing environment, changes in technologies, or the discovery of new vulnerabilities in what had been considered “safe” products may lead to additional security controls.

**Perform Controls Analysis**: An analysis of identified controls is conducted to determine their potential effectiveness to remove, transfer, or otherwise mitigate risk to the information resource. The controls analysis identifies any residual risk to the information resource.

**Perform Cost Benefit Analysis**: A cost benefit analysis is performed and documented to facilitate the implementation of cost-effective protection for information resources and continuity of business operations.

### 4-3.4.4 Develop Security Plan

#### 4-3.4.4.1 General

A security plan must be developed for sensitive-enhanced, sensitive, and critical information resources. A security plan is also required for major information resources and general support systems.

A security plan is a blueprint for protecting the information resource against threats, both internal and external. The security plan covers both the development and production environment. The plan describes all information security controls and processes that have been implemented or planned and

delineates responsibilities and expected behavior of all individuals who access the information resource.

The security plan documents the security requirements identified in the BIA and the information security controls that are tailored to the security requirements. The Security Plan template and instructions for completing are available on the IT Web site. Select TSLC; under the Analysis and Design Phase, select Information Resource Security Plan.

#### 4-3.4.4.2 Security Plan Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Executive sponsor | Provides personnel and financial resources to supports development of a security plan. |
| Portfolio manager | Provides guidance and assistance. |
| ISSR | Support executive sponsor and portfolio manager as requested. |
| ISSO | Provides guidance and consulting support and coordinates completion of the security plan. |
| Development team | Defines specific security controls and processes, completes security plan, and keeps C&A core team informed of progress. |

### 4-3.4.5 Assess Risks

A risk assessment must be conducted for all information resources to identify security concerns (e.g., threats, vulnerabilities, and control weaknesses), risk ranking, additional controls, and residual risk.

Risk analysis is a continual process throughout this phase; it depends on the configuration of the information resource, the users, and the implementation environment. Risks to information resources and facilities are evaluated with the following processes:

a. Risk assessment.

b. Site security review (conducted by an ISSO and the Postal Inspection Service).

c. External independent information security risk assessment (if requested).

Standard templates and worksheets that serve as a framework for the risk assessments are incorporated in the risk assessment processes.

### 4-3.4.6 Conduct Risk Assessment

The risk assessment is an ongoing process designed to minimize risk to information resources by identifying additional security controls (i.e., beyond those initially established) to be deployed that are commensurate with the relative values of the assets to be protected, the vulnerabilities associated with those assets, and threats to the information resource. The risk assessment template and instructions for completing them are available on the IT Web site. Select TSLC; under the Analysis and Design Phase, select Risk Assessment.

#### 4-3.4.6.1 Risk Assessment Activities

A risk assessment will do the following:

a. Identify general administrative data and assets.
b. Identify possible threats that could adversely affect the information resource.
c. Identify security vulnerabilities that could be exploited by threat events affecting the information resource.
d. Analyze implemented and planned controls against requirements.
e. Identify the probability that a vulnerability may be exploited.
f. Identify the adverse impact resulting from a successful exploitation of a vulnerability.
g. Determine the overall risk to the information resource.
h. Identify possible additional mitigating controls that, if applied, could be expected to mitigate the risks identified for the information resource.
i. Document the overall risk status of the information resource.

#### 4-3.4.6.2 Risk Assessment Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Executive sponsor | Ensures completion of the risk assessment for information resources under their purview.<br>Provides personnel and financial resources to support risk assessment activities. |
| Portfolio manager | Supports executive sponsor as requested. |
| ISSR | Supports executive sponsor as requested. |
| ISSO | Provides guidance on applicability of threats or vulnerabilities and appropriate choice of countermeasures; coordinates completion of risk assessment. |
| Development team | Completes risk assessment and keeps C&A core team informed of progress. |
| VP IT Solutions and VP of functional business area | Jointly accepts any residual risk associated with information resource. |

### 4-3.4.7 Conduct Site Security Review

The site security review assesses the physical security controls of facilities hosting sensitive-enhanced, sensitive, and critical information resources. The lack of adequate physical security controls could affect the availability, confidentiality, and integrity of Postal Service information resources.

All business partner sites connecting to a Postal Service information infrastructure are subject to a site security review performed by the manager CISO and the Chief Inspector, or their designees. A site security review must be conducted if a facility is hosting enhanced sensitive, sensitive, or critical information resources. A site security review may be conducted at any time as long as connectivity exists between the business partner and Postal.

### 4-3.4.7.1 Site Security Review Areas

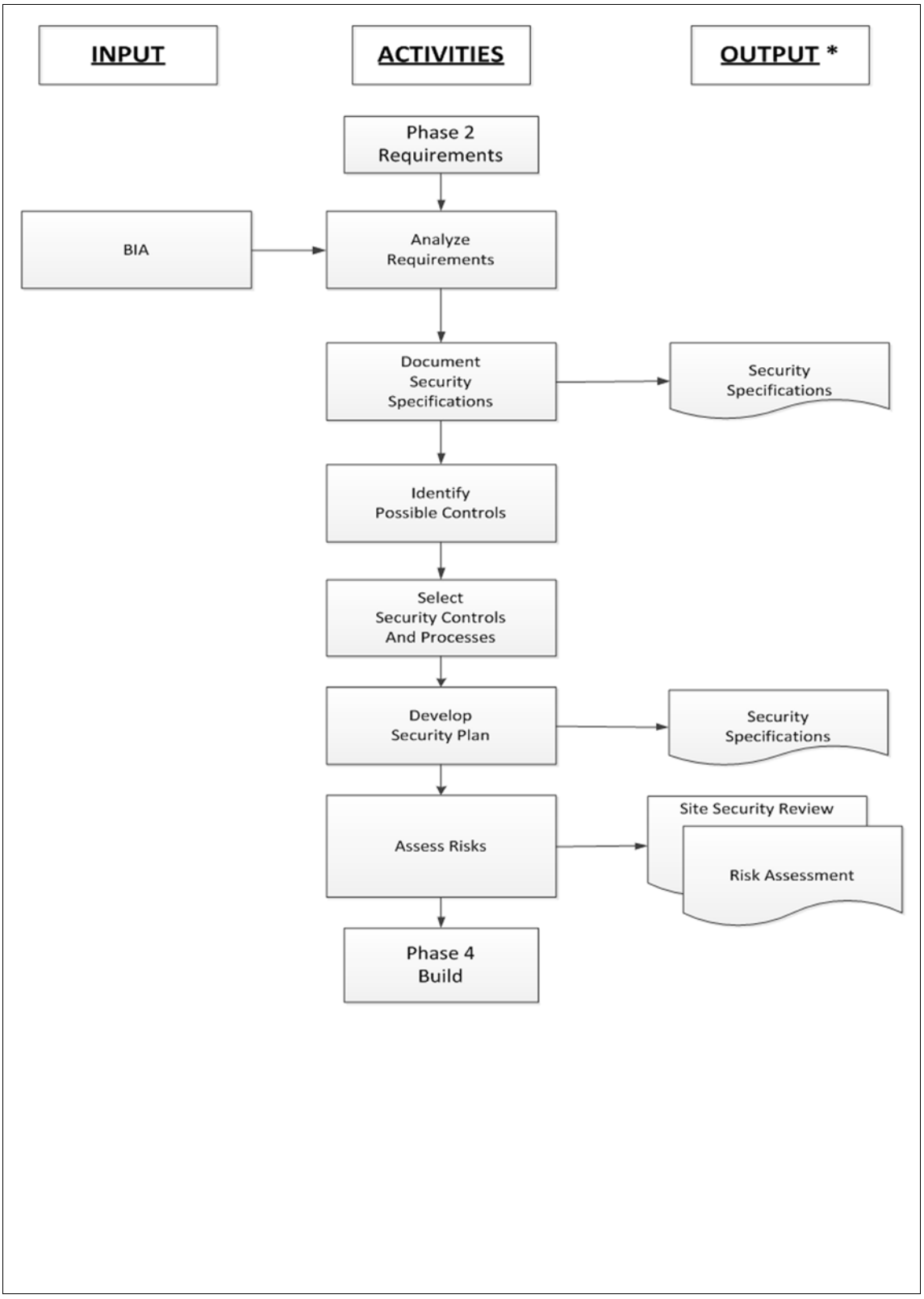
The site security review evaluates risks in the following areas as they relate to the physical security of applications and the information resources hosting them:

a. Location security.
b. Facility security.
c. Personnel security.
d. Controlled area security.
e. Environmental security.
f. Communications security.
g. Hardware security.
h. Software security.
i. Information security.
j. Administrative security.
k. Emergency response and contingency planning.
l. Auditing and monitoring.

### 4-3.4.7.2 Site Security Review Roles and Responsibilities

The Inspection Service and the ISSO complete the site security review.

Exhibit 4-3
**Phase 3, Design**



# 4-4 Phase 4 — Build

Phase 4 develops, acquires, and integrates security controls. (See Exhibit 4-4, Phase 4, Build.)

## 4-4.1 Objectives

The objectives for this phase are as follows:

a. Developing, acquiring, and integrating security controls.
b. Hardening servers
c. Developing standard operating procedures.
d. Developing operational training materials.
e. Incorporating security requirements in service level agreement (SLA) and trading partner agreement (TPA), if applicable.
f. Registering information resource in eAccess.
g. Initiating contingency recovery planning.
h. Submitting an NCRB request, if applicable.
i. Reassess threats, vulnerabilities, and risks.

## 4-4.2 Deliverables

The deliverables for this phase are the following:

a. Standard operating procedures.
b. Operational training materials.
c. SLA and TPA, if applicable.
d. Draft contingency planning documents. (The contingency planning documents are started during this phase.)
e. NCRB request, if applicable.
f. Updated risk assessment.

## 4-4.3 Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Executive sponsor | Ensures completion of Phase 4 activities. |
| Portfolio manager | Provides guidance and assistance. |
| ISSR | Supports executive sponsor as required. |
| ISSO | Provides guidance and consulting support for completion of C&A deliverables. |
| Development team | Completes C&A deliverables and keeps C&A core team informed of progress. |
| DRS | Consults with executive sponsor as required on the development of contingency planning documents. |

## 4-4.4 Activities

### 4-4.4.1 Develop, Acquire, and Integrate Information Security Controls

A member of the C&A core team serves as the liaison between the executive sponsor and the development team on the required information security controls and processes. The development team acquires, builds, and integrates these controls and processes and keeps the C&A core members informed of their progress.

### 4-4.4.2 Harden Information Resources

Information resources hosting applications designated as sensitive-enhanced, sensitive, or critical must be hardened to meet or exceed the requirements documented in Postal Service hardening standards. Hardening refers to the process of implementing additional software, hardware, or physical security controls.

### 4-4.4.3 Develop Standard Operating Procedures

Standard operating procedures (SOPs) must be developed for information resources designated as sensitive-enhanced, sensitive, or critical to handle the operating support required for the information resource. These procedures cover such topics as separation of duties, manual processes, computer operations, input and output validation, and report distribution.

### 4-4.4.4 Develop Operational Security Training Materials

Appropriate materials must be developed for training users, system administrators, managers, and other personnel on the correct use of the information resource and its security controls.

### 4-4.4.5 Incorporate Security Requirements in Service Level Agreements and Trading Partner Agreements

Service level agreements (SLAs) are often developed for in-house managed and/or developed information resources. Trading partner agreements (TPAs) are often developed for externally managed and/or developed information resources. If SLAs or TPAs are developed, incorporate information security requirements.

### 4-4.4.6 Register Information Resources in eAccess

The information resource must be registered in eAccess, which is the Postal Service's application for managing the authorization process for personnel needing to access an information resource and the associated information. Registration is also required for the use of managed accounts (i.e., machine accounts, etc.).

### 4-4.4.7 Initiate Contingency Planning

If the BIA determines that contingency planning is required based on the criticality determination, it should be initiated at this stage. Contingency planning continues throughout the life cycle of the information resource.

### 4-4.4.7.1 Contingency Planning Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Executive sponsor | Consults with the DRS on the contingency planning documents, the recovery time objective (RTO), and recovery point objective (RPO).<br>Coordinates with other managers in planning contingency planning activities.<br>Fund information resource contingency planning activities. |
| Portfolio manager | Provide guidance and assistance. |
| ISSR | Support executive sponsor and portfolio manager as requested. |
| ISSO | Provide guidance and consulting support. |
| Development Team | Develop and maintain the contingency planning documents. |
| DRS | Consult with the executive sponsor on the contingency planning documents and validates the RTO and RPO, based on overall Postal Service resources, to ensure it is realistic and achievable. |

### 4-4.4.7.2 Develop Contingency Planning Documents

Contingency planning documents are required for information resources designated as critical (i.e., high or moderate). The development of the contingency planning documents is begun during Phase 4 in coordination with the DRS. Contingency plans are tested and updated in Phase 7. Contingency planning templates are available on the IT Web site. Select Corporate Information Security, select Business Continuance Management page, select Business Continuance Management, and then select Business Continuance Management documents.

The Application Disaster Recovery Plan (ADRP) is a primary component of contingency planning. An ADRP is required for applications designated as critical.

## 4-4.4.8 Identify Connectivity Requirements

Identify connectivity requirements and submit a request to the Network Connectivity Review Board (NCRB).

## 4-4.4.9 Reassess Threats, Vulnerabilities, and Risks

As development or integration proceeds, requirements may change. Planned security controls and processes may be less effective than what is needed when the entire information resource environment is considered or may be unable to be implemented because of costs, supporting resources, or available technology. Such changes may affect the risk to the information resource and the Postal Service. A reassessment may indicate, however, that no changes to the planned security controls, the security plan, or the risk assessment are required.

Exhibit 4-4
**Phase 4, Build, (p. 1 of 2)**

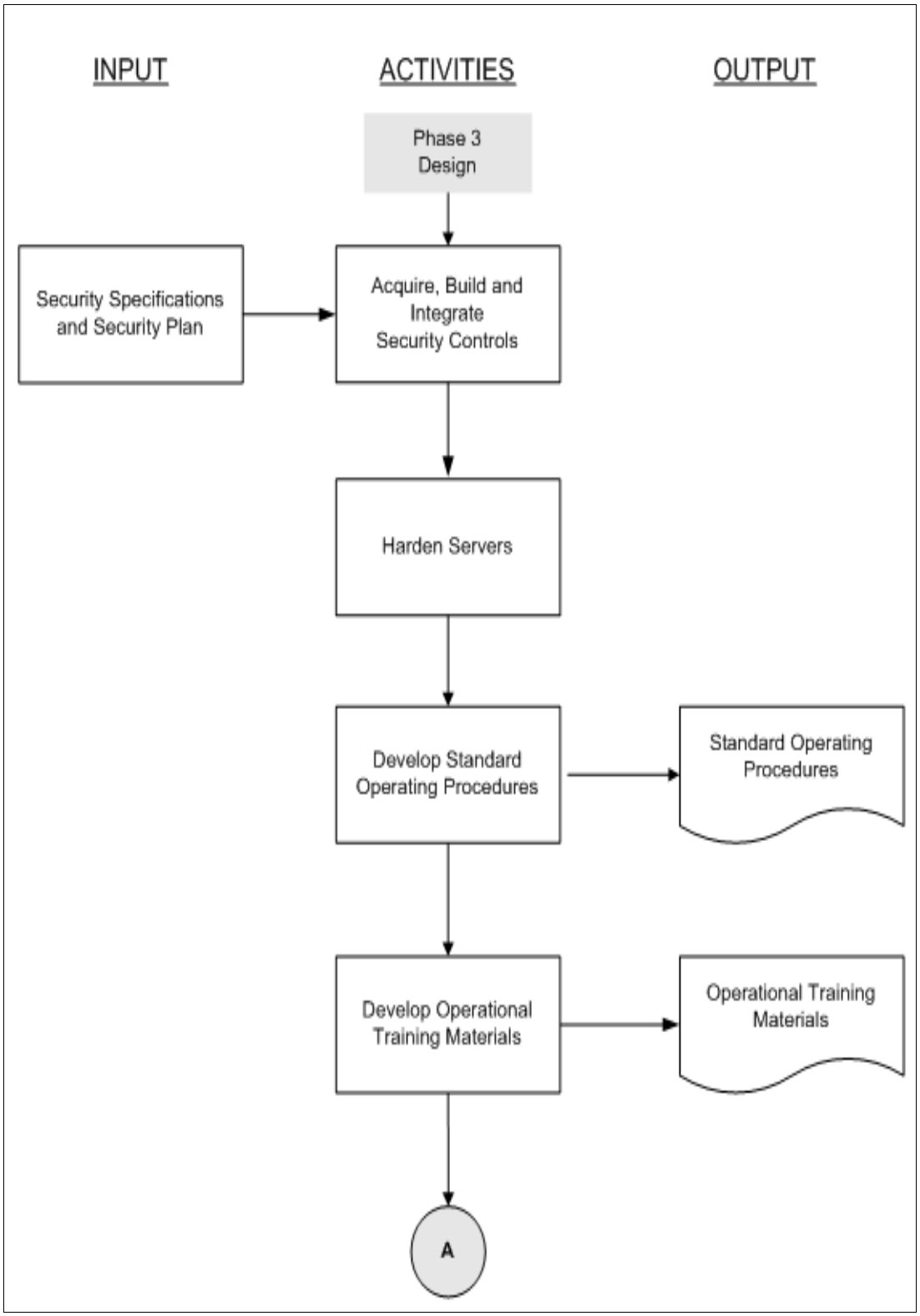
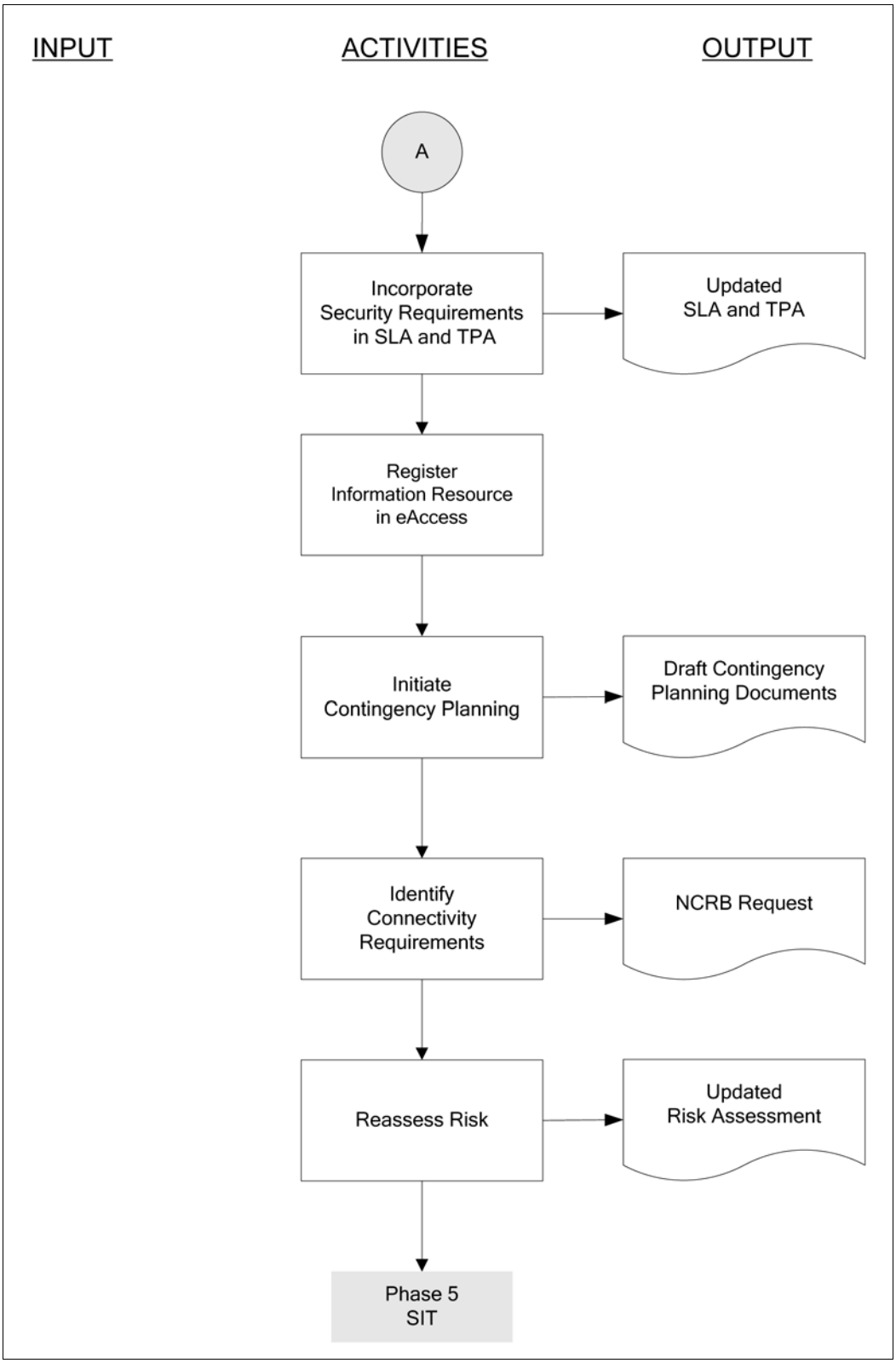


Exhibit 4-4
**Phase 4, Build, (p. 2 of 2)**



# 4-5 Phase 5 – System Integration Testing

Phase 5 focuses on testing the security controls and processes acquired, built, and integrated in the Build Phase to determine their effectiveness. (See Exhibit 4-5, Phase 5, System Integration Testing.)

## 4-5.1 Objectives

The objectives of this phase are as follows:

a. Developing a security test and evaluation (ST&E) plan.

b. Conducting operational security training.

c. Completing the development of contingency plans.

## 4-5.2 Deliverables

The deliverables in this phase are the following:

a. ST&E plan.

b. Documentation indicating operational security training was conducted.

c. Contingency plans.

## 4-5.3 Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Executive sponsor | Ensures completion of Phase 5 activities. |
| Portfolio manager | Provides guidance and assistance. |
| ISSR | Supports executive sponsor and portfolio manager as requested. |
| ISSO | Provides guidance and consulting support for completion of C&A deliverables. |
| Development team | Develop ST&E plan, conduct and document operational security training, and develop contingency plan. |

***Note:*** If the projected delivery dates of the ST&E plan, operational security training, or contingency plan change, the POA&M must be amended and the ISSO notified of the changes.

## 4-5.4 Activities

### 4-5.4.1 Develop Security Test and Evaluation Plan

#### 4-5.4.1.1 General

A ST&E plan must be developed for information resources designated as sensitive-enhanced, sensitive, or critical. A security test and evaluation plan is also required for major information systems and general support systems.

The ST&E plan defines the security testing to be conducted to determine the extent to which the information resource meets the security requirements for its mission and operational environment. If the ST&E plan is part of an overall system test plan, highlight or flag the security section for ease of review.

Sensitive-enhanced and sensitive test data should be protected throughout the entire testing cycle.

#### 4-5.4.1.2 Build Security Test and Evaluation Plan

The development team should build the ST&E plan and include the stakeholders in the process. The Security Test and Evaluation template and instructions are available on the IT Web site. Select TSLC Templates; under System Integration Test, select Security Test and Evaluation Plan. The ST&E plan should do the following:

a. Address all security controls and processes described in the security plan and the means by which those controls and processes will be tested.
   (1) Include both the technical and nontechnical security controls.
   (2) Include controls associated with hardware, operating system, networking and telecommunications, physical security, personnel security, and computer operations, and manual processes.

b. Define the security functionality (security control feature) to be tested for each security control implemented to satisfy the security requirement.

c. Describe the actual testing to be performed for each control. For each control, include applicable test scripts, scenarios, performance thresholds, and an indication of what will constitute passing or failing.

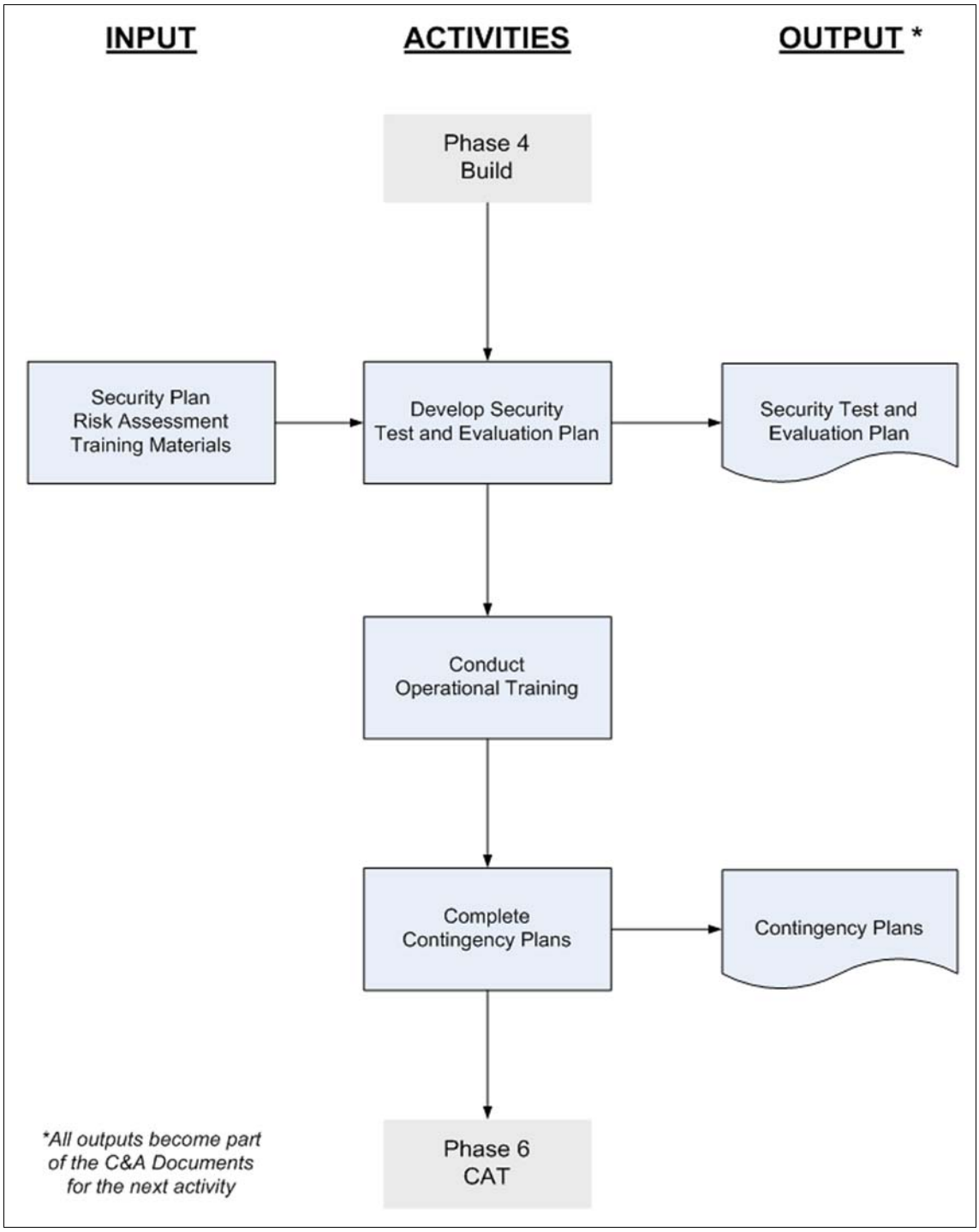
### 4-5.4.2 Conduct Operational Security Training

Using the training materials developed in phase 3, train users, system administrators, management, and other personnel on the correct use of the information resource and its security safeguards.

### 4-5.4.3 Complete Contingency Planning

Contingency planning documents are required for information resources designated as critical. The development of the contingency planning documents is begun during Phase 4 in coordination with the DRS and updated in this phase.

Exhibit 4-5
**Phase 5, SIT**



# 4-6 Phase 6 – Customer Acceptance Testing

Phase 6 consists of those activities that culminate in certification, a risk mitigation plan, and accreditation. (See Exhibit 4-6, Phase 6, CAT.)

## 4-6.1 Objectives

The objectives of this phase are as follows:

a. Conducting security code review, if applicable.
b. Conducting security testing and documenting the results.
c. Conducting vulnerability scans.
d. Conducting independent reviews, if applicable.
e. Addressing any outstanding issues, if applicable.
f. Completing the certification and accreditation evaluation report.
g. Certifying the information resource.
h. Developing a risk mitigation plan.
i. Accepting the residual risk.
j. Accrediting the information resource.

## 4-6.2 Deliverables

The deliverables of this phase are the following:

a. Security code review, if applicable.
b. ST&E report.
c. Vulnerability scans.
d. Independent reviews, if applicable.
e. List of outstanding issues, if applicable.
f. Certification and Accreditation Evaluation Report.
g. Certification Letter.
h. Risk Mitigation Plan.
i. Acceptance of Risk Responsibility Letter.
j. Accreditation Letter.

## 4-6.3 Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Development team | Request code review (if applicable), conduct security testing, document security testing, request vulnerability scans, request independent reviews (if applicable), and develop list of outstanding items (if applicable). |
| ISSO | Evaluates C&A documentation, prepares an C&A evaluation report that details the findings, makes the decision to escalate security concerns or signs the C&A evaluation report and forwards the report and the C&A documentation package to the certifier. |
| Certifier (program manager C&A process) | Reviews the C&A evaluation report and C&A documentation package, makes the decision to escalate security concerns or certifies the information resource by preparing and signing a certification letter, and forwards the certification letter and C&A documentation package to the portfolio manager. |
| Portfolio manager | Analyzes C&A and business documentation, makes the decision to escalate security concerns or prepares a risk mitigation plan addressing high and medium risks and recommending whether the risks should be accepted, transferred, or further mitigated. If a documented vulnerability will not be mitigated, prepares and signs an acceptance of responsibility letter and forwards the risk mitigation plan and C&A documentation package to the accreditor. |
| Accreditor (manager, CISO) | Analyzes C&A and business documentation, makes the decision to escalate security concerns, or prepares and signs an accreditation letter. Forwards the accreditation letter and C&A documentation package to the executive sponsor and portfolio manager. |
| Executive sponsor | Ensures completion of C&A process and provides personnel and financial resources for correcting deficiencies. |
| ISSR | Supports executive sponsor and portfolio manager as requested to correct deficiencies. |
| Other stakeholders | Participate by responding on outstanding issues or providing advisory support. |

***Note:*** If the projected delivery dates of the security code review (if applicable), ST&E testing and report, vulnerability scans, independent reviews (if applicable), or list outstanding items (if applicable) change, the POA&M must be amended and the ISSO notified of the changes.

## 4-6.4 Activities

### 4-6.4.1 Conduct Security Code Review

To protect the infrastructure, a documented security code review is required for:

a. Any externally facing or DMZ-hosted information resource containing custom programming or scripting, regardless of the designation of sensitivity or criticality.

b. Information resources designated as sensitive-enhanced, sensitive, and critical that contain dynamic code or COTS custom programming or scripts.

c. Internally and externally facing PCI applications containing customs code. The code review can be conducted by a knowledgeable independent individual or by a third-party vendor.

The security code review will be (1) based on the Postal Service Information Security Code Review Standards or an acceptable equivalent, and (2) appropriately documented. This security code review will not be required if an independent security code review is conducted. (See 5-1, Independent Security Code Review.)

## 4-6.4.2 Conduct the Security Test and Evaluation

### 4-6.4.2.1 Conduct Security Test Process

Security testing must be conducted for information resources designated as sensitive-enhanced, sensitive, or critical. Security testing is also required for major information system and general support systems. Some types of testing include network scanning, vulnerability scanning, penetration testing, password cracking, log reviews, file integrity testing, virus detection, war dialing, and war driving.

The executive sponsor must ensure that security testing is conducted using the approved ST&E plan. Following the ST&E plan reduces the risk of false or faulty test results; yields more consistent, comparable, and repeatable evaluation of security controls; and results in more complete and reliable information for authorizing officials.

The information resource technical control mechanisms and the surrounding administrative controls are evaluated to establish the extent to which the information resource meets the security requirements.

The executive sponsor collaborates with stakeholders (who may include, but are not limited to, the ISSO, ISSR, developers, and contractors) to determine their participation in the testing.

If a modification to a control is required, the change should be reflected in the security plan and the ST&E plan before the test is re-executed.

### 4-6.4.2.2 Develop Security Test and Evaluation Report

Upon completion of the testing, the development team and executive sponsor have the following responsibilities:

a. The development team develops a ST&E report and submits the findings to the executive sponsor. If the ST&E report is a part of an overall test report, highlight or flag the section addressing information security testing for ease of review.

b. The executive sponsor, in collaboration with the ISSO, reviews the findings and determines whether the security controls and processes are adequate to protect the information resource or whether modifications to the security controls and processes are warranted. If modifications are warranted, the security plan and the ST&E plan are amended and testing reinitiated.

### 4-6.4.3 Conduct Vulnerability Scans

Vulnerability scans are recommended for all information resources and are required for the following information resources:

a. Annually for externally facing information resources.

b. Quarterly for PCI information resources (i.e., information resources utilizing credit card transactions).

Scanning procedures must ensure adequate scan coverage and the updating of the list of vulnerabilities to be scanned for.

### 4-6.4.4 Conduct Independent Reviews

The following independent reviews may be required during Phase 3 to determine the effectiveness of the security controls and processes:

a. Independent security code reviews.

b. Independent risk assessments.

c. Independent penetration testing and vulnerability scans.

d. Independent security test validations.

These reviews are discussed in Chapter 5, Independent Reviews.

### 4-6.4.5 Address and Resolve Outstanding Issues

Outstanding issues are addressed and resolved. If an outstanding issue cannot be resolved, the information resource C&A Phase should be revisited.

### 4-6.4.6 ISSO Evaluates C&A Documentation

The ISSO initiates the evaluation of the C&A documentation package early in the C&A process. This enables the C&A core team to be proactive in identifying and addressing information security concerns. The C&A documentation package includes:

a. BIA.

b. Architecture diagram.

c. Security specifications.

d. Security plan.

e. SOPs.

f. SLAs or TPAs, if applicable.

g. Risk assessment.

h. ST&E plan.

i. ST&E report.

j. POA&M.

k. Code review, if applicable.

l. Vulnerability scans, if applicable.

m. Independent reviews, if applicable.

### 4-6.4.7 ISSO Prepares C&A Evaluation Report

Upon completion of the evaluation, the ISSO prepares a C&A evaluation report that details the results.

### 4-6.4.8 ISSO Escalates Security Concerns or Forwards C&A Package

Upon completion of the C&A evaluation report, the ISSO escalates security concerns or signs the C&A evaluation report and forwards the report and supporting documentation to the certifier (manager, C&A process) for review.

If the ISSO decides not to proceed with certification, he or she will indicate the C&A Phase to return to for rework.

### 4-6.4.9 Certifier Escalates Security Concerns or Certifies Information Resource

The certifier (program manager, C&A process) reviews the C&A evaluation report and the supporting C&A documentation package, escalates security concerns or prepares and signs a certification letter, and forwards the certification letter and C&A documentation package to the portfolio manager.

If the certifier decides not to certify the information resource, he or she will indicate the C&A Phase to return to for rework.

### 4-6.4.10 Portfolio Manager Escalates Security Concerns or Prepares Risk Mitigation Plan and Acceptance of Responsibility Letter (if Required)

The portfolio manager reviews the certification letter, the supporting C&A and business documentation, and escalates security concerns or prepares a risk mitigation plan for any residual risks rated as medium or high.

Risk mitigation strategies include the following:

a. Risk assumption: The portfolio manager assumes the risk.

b. Risk avoidance: The portfolio manager recommends that the portion of the project that is causing the risk exposure should not be implemented as planned or at this time.

c. Risk limitation: The portfolio manager limits the exposure to the threat (e.g., limit the number of users with privileged access or implement two-factor authentication).

d. Risk planning: The portfolio manager concedes that the Postal Service will have to accept a certain amount of loss in order to take advantage of the increased functionality or income associated with the information resource. The risk planning will define the acceptable amount of loss.

e. Acknowledgement and research: Acknowledge the risk and conduct research into appropriate cost-effective controls that can be implemented in the future.

f. Implement additional controls to further mitigate the risks.

g. Risk transfer: Transfer the risk to another organization (e.g., business partner).

If a documented vulnerability associated with the medium or high residual risk will not be mitigated, the portfolio manager prepares and signs an acceptance of risk responsibility letter and then forwards it, the risk mitigation plan, and C&A documentation package to the accreditor.

If the portfolio manager decides not to (1) sign the acceptance of risk responsibility letter, or (2) proceed with accreditation, he or she will indicate the C&A Phase to return to for rework.

### 4-6.4.11 Accreditor Escalates Security Concerns or Accredits Information Resource

The accreditor (manager, CISO) reviews the risk mitigation plan and the supporting C&A documentation, escalates security concerns or prepares and signs an accreditation letter, and forwards the accreditation letter and final C&A documentation package to the executive sponsor and portfolio manager.

If the accreditor decides not to accredit the information resource, he or she will indicate the C&A Phase to return to for rework.

Exhibit 4-6
**Phase 6, CAT, (p. 1 of 3)**

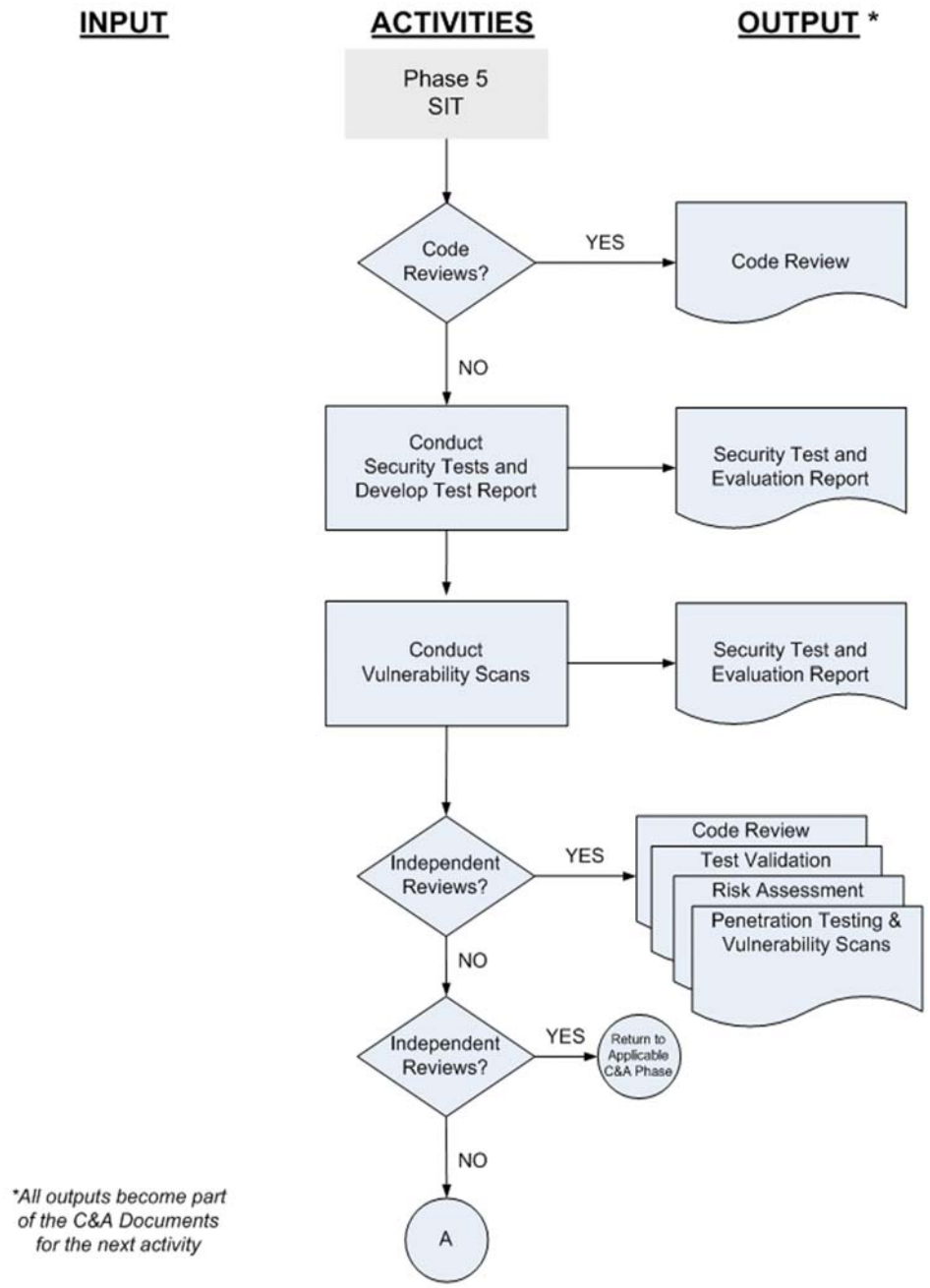


Exhibit 4-6
**Phase 6, CAT, (p. 2 of 3)**

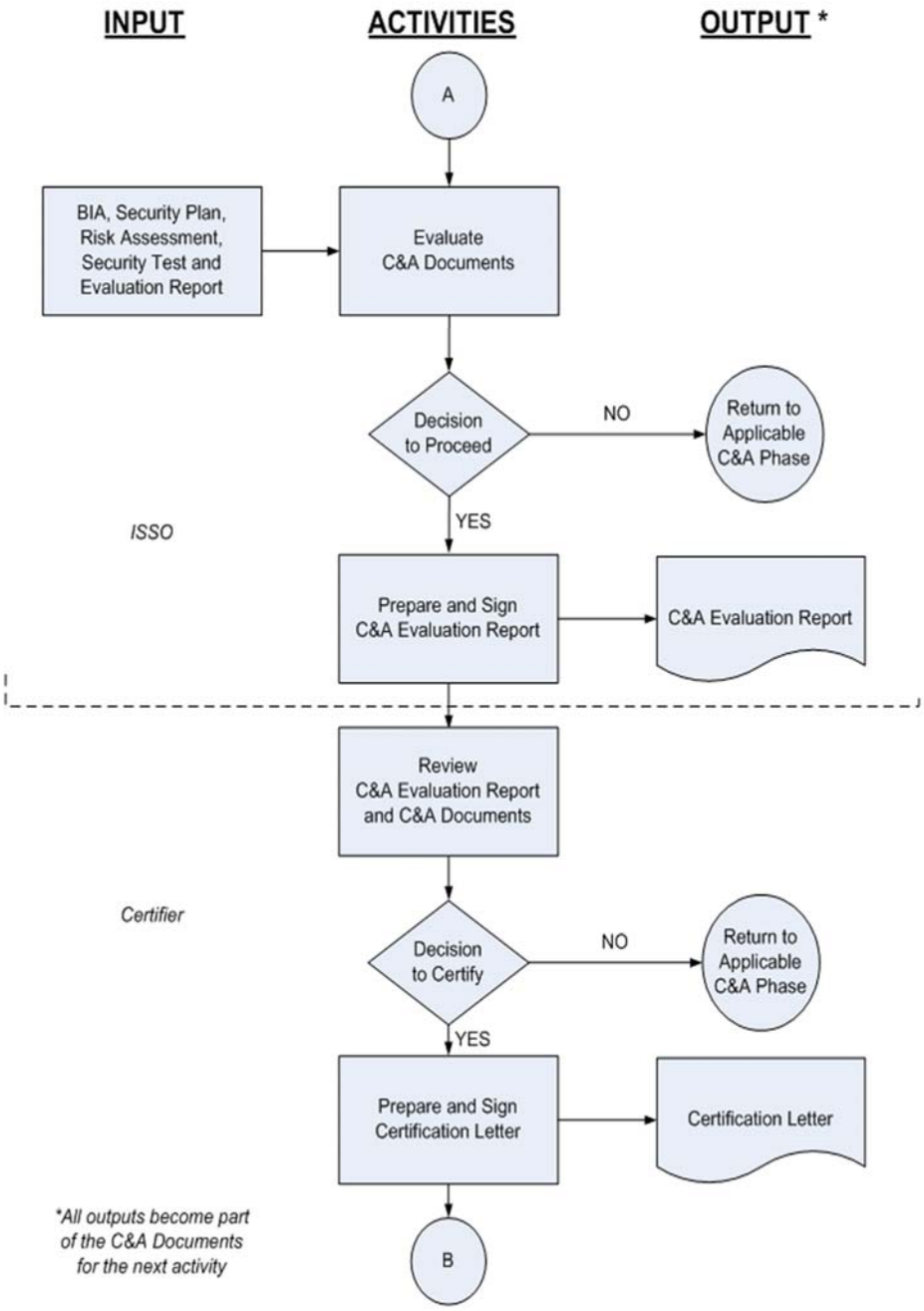
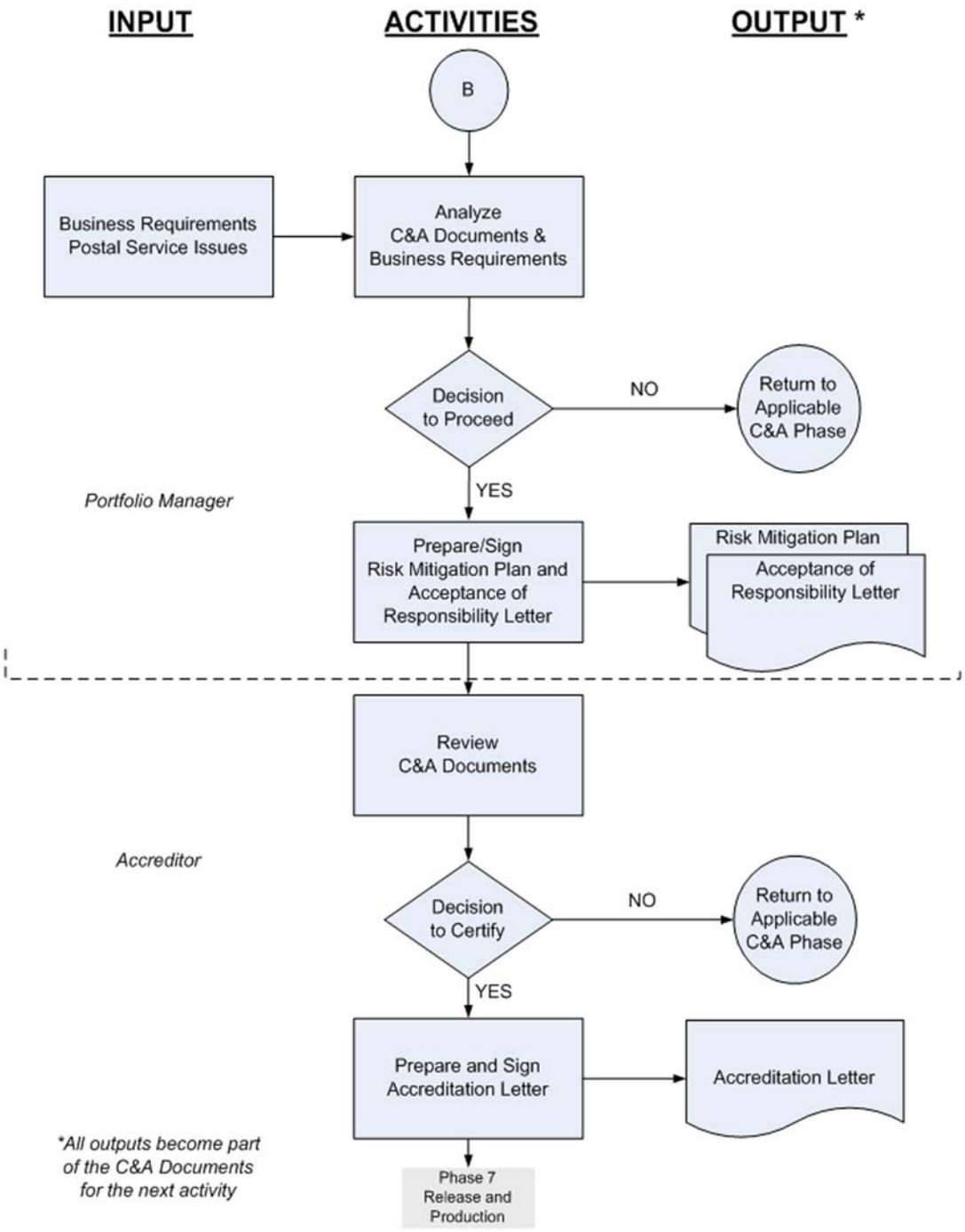


Exhibit 4-6
**Phase 6, CAT, (p. 3 of 3)**



# 4-7 Phase 7 – Release and Production

Phase 7 deploys the information resource and encompasses activities that occur after the information resource is deployed to the production environment and continue throughout the remainder of the information resource life cycle. (See Exhibit 4-7, Phase 7, Release and Production.) These activities include operations, maintenance, and retirement.

## 4-7.1 Objectives

The objectives of this phase are as follows:

a. Deploying the information resource.

b. Testing contingency plans.

c. Protecting the information resource after deployment and throughout its life cycle.

d. Reinitiating the C&A Process as required.

e. Retiring the information resource at the end of its life cycle.

## 4-7.2 Deliverables

The deliverables for this phase are the following:

a. Deployment letter

b. Revised C&A documentation.

c. Contingency planning test results and lessons learned.

## 4-7.3 Roles and Responsibilities

| Roles | Responsibilities |
|---|---|
| Executive sponsor and portfolio manager as agents of the VP functional business area and VP IT Solutions, respectively | Jointly review C&A and business documentation and make the decision to return the information resource to the applicable C&A phase for rework or to deploy it into the production environment by preparing and signing a deployment letter. |
| Project manager | Deploys the information resource and files the C&A documentation package.<br>With DRS, ensures that the contingency plans are tested periodically and the test results and lessons learned documented.<br>Ensures that the contingency planning documents are updated and maintained current.<br>Ensures that C&A documentation package is kept current.<br>Ensures the secure operations and maintenance of information resource.<br>Ensures that the existing security controls are periodically reviewed to determine whether they are still sufficient and implements additional security controls or modifies existing security controls as required. |
| Executive sponsor | Determines whether changes are significant and ensures that the C&A process is reinitiated as required.<br>Retires the information resource when no longer needed. |
| Portfolio manager | Provides guidance and assistance. |

| Roles | Responsibilities |
|---|---|
| ISSR | Supports executive sponsor and portfolio manager as requested. |
| ISSO | Provides guidance and consulting support. |
| DRS | Reviews contingency planning documents and accepts them as complete or returns them to the executive sponsor for rework.<br>Stores the contingency planning documents.<br>With the project manager, tests the contingency plans. |

## 4-7.4 Activities

### 4-7.4.1 Executive Sponsor and Portfolio Manager Make Decision to Deploy (or Continue to Deploy) or Return for Rework

The executive sponsor and portfolio manager review the accreditation letter, risk mitigation plan, and supporting C&A documentation package. They will issue a joint decision on whether to deploy the information resource and with what restrictions, if any. If they decide to approve and deploy, they will prepare and sign a deployment letter.

If they decide not to approve deployment, they will indicate the C&A Phase to return to for rework.

### 4-7.4.2 Data Conversion

If required, a data conversion plan is defined which incorporates collecting, converting, and verifying data for completeness and integrity and resolving any errors found during conversion. A backup of all data is created prior to conversion, audit trails track the conversion, and there is a fallback and recovery plan in case the conversion fails. The backed up data conforms to the applicable data retention schedule.

### 4-7.4.3 Deploy Information Resource

All four approvals (i.e., certification, accreditation, risk acceptance, and approval to deploy) are required before deploying the information resource. The project manager deploys the information resource into production with the security controls documented in the security plan and tested in the ST&E and with any restrictions documented in the approval letters. The project manager files the C&A documentation package.

### 4-7.4.4 Operate Information Resource

The information resource is operated with the security controls, processes, and procedures in place as documented in the security plan, ensuring that they remain fully functional and unaltered by maintenance procedures.

***Note:*** To use production data in a test environment, you must have prior written approval (see Section 8-3.3, Testing Restrictions, in Handbook AS-805, *Information Security*, for specific requirements).

### 4-7.4.5 Test Information Resource Contingency Plans

The information resource contingency plans are tested and the test results and lessons learned are documented.

### 4-7.4.6 Maintain Information Resource

The information resource is placed under configuration control and all changes are documented.

The tools, techniques, and mechanisms used to maintain information resources must be properly controlled.

### 4-7.4.7 Reassess Risks and Upgrade Security Controls

Risks must be re-assessed any time significant changes are made to the information resource, if a serious security breach occurs, if significant audit findings regarding security are issued, at the request of management, or as part of the re-initiation of the C&A process.

### 4-7.4.8 Monitor Operations and Enhance Security Posture

Information resource controls must be continually monitored to:

a. Ensure the controls are working as intended.

b. Ensure changes are controlled and documented in the configuration and change management system.

c. Ensure the operating environment (e.g., physical, electronic, political, legal) has not introduced new vulnerabilities.

d. Determine whether additional security controls need to be added or existing controls modified to properly secure the information resource in the changing environment.

e. Ensure the information resource remains in compliance with the security-related plans and Postal Service information security policies.

Facility and platform related controls must also be monitored for compliance with Postal Service policies.

If the information resource security posture or controls change significantly, it is necessary to re-initiate the C&A process.

### 4-7.4.9 Periodically Test Security Controls

A subset of the information resource information security controls must be formally tested annually, the tests documented, and the results submitted to the ISSO. The security controls that are volatile or critical to protecting the information resource must be assessed at least annually. All other controls must be assessed at least once during the information resource's accreditation cycle (e.g., for those information resources on a 3-year cycle test one third of the other controls each year and for those information resources on a 5-year cycle test one fifth of the other controls each year).

### 4-7.4.10 Update Certification and Accreditation Documentation Package

The C&A documentation package (including the Security Plan and Security Test and Evaluation Plan) must be updated throughout the life cycle process in response to the changing environment, changing technology, reassessed risks or vulnerabilities, and as part of the re-initiation of the C&A process. See Exhibit 4-7.4.10a, C&A Templates and Exhibit 4-7.4.10b, C&A Requirements for Information Resources.

### 4-7.4.11 Re-initiate C&A as Required

Re-initiating the C&A is required based on the information resource classification designation.

Re-initiating the C&A is also required for a significant change to the information resource, including new business requirements or a change to the information resource's level of criticality or sensitivity, a significant audit finding, a significant security incident, or a request by management.

Unresolved issues, new business requirements, new threats and vulnerabilities, operating environment changes, audit reports, and incidents must be appropriately addressed throughout the information resource life cycle. Also, certain changes to an information resource or its environment as well as business considerations could affect the security of the information resource and may require a re-initiation of the C&A process. (See Chapter 6, Re-Initiating the C&A for specific criteria.)

### 4-7.4.12 Dispose of Sensitive-Enhanced or Sensitive Data

Postal Service sensitive-enhanced or sensitive information that is no longer needed, whether in electronic or nonelectronic format, must be transferred, archived, or destroyed in accordance with official Postal Service policies and procedures.

### 4-7.4.13 Dispose of Equipment and Media

Postal Service hardware and media containing sensitive-enhanced or sensitive information that is no longer needed must be completely erased (sanitized) or destroyed prior to disposal.

### 4-7.4.14 Retire Information Resource

Information resources may eventually be retired. Upon determination that an information resource has reached the end of its life cycle, the executive sponsor ensures all data is completely removed from the assets being retired and retires the information resource in accordance with Handbook AS-805, *Information Security*.

Exhibit 4-7
**Phase 7 Release and Production, (p. 1 of 3)**

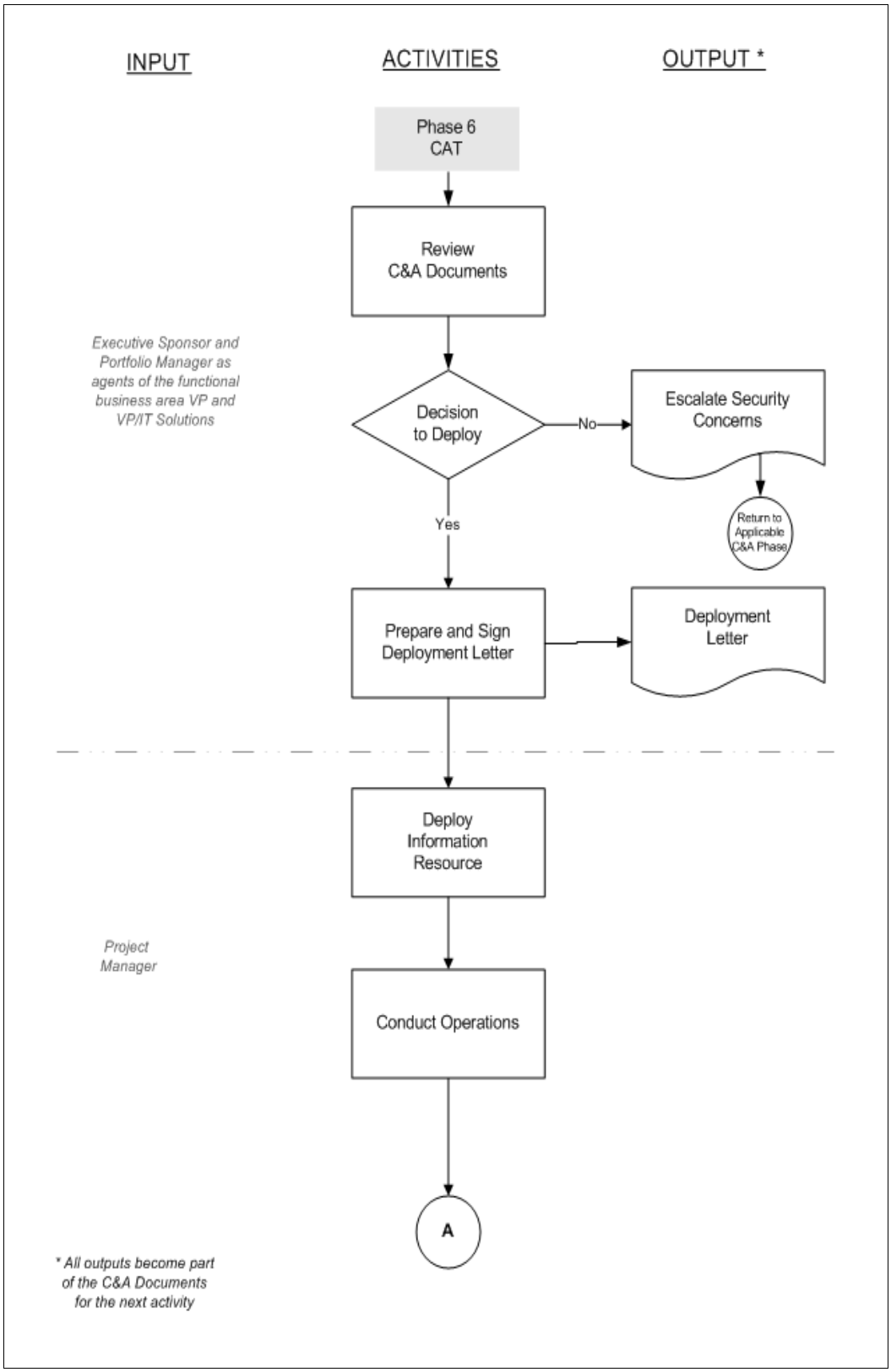


Exhibit 4-7
**Phase 7 Release and Production, (p. 2 of 3)**

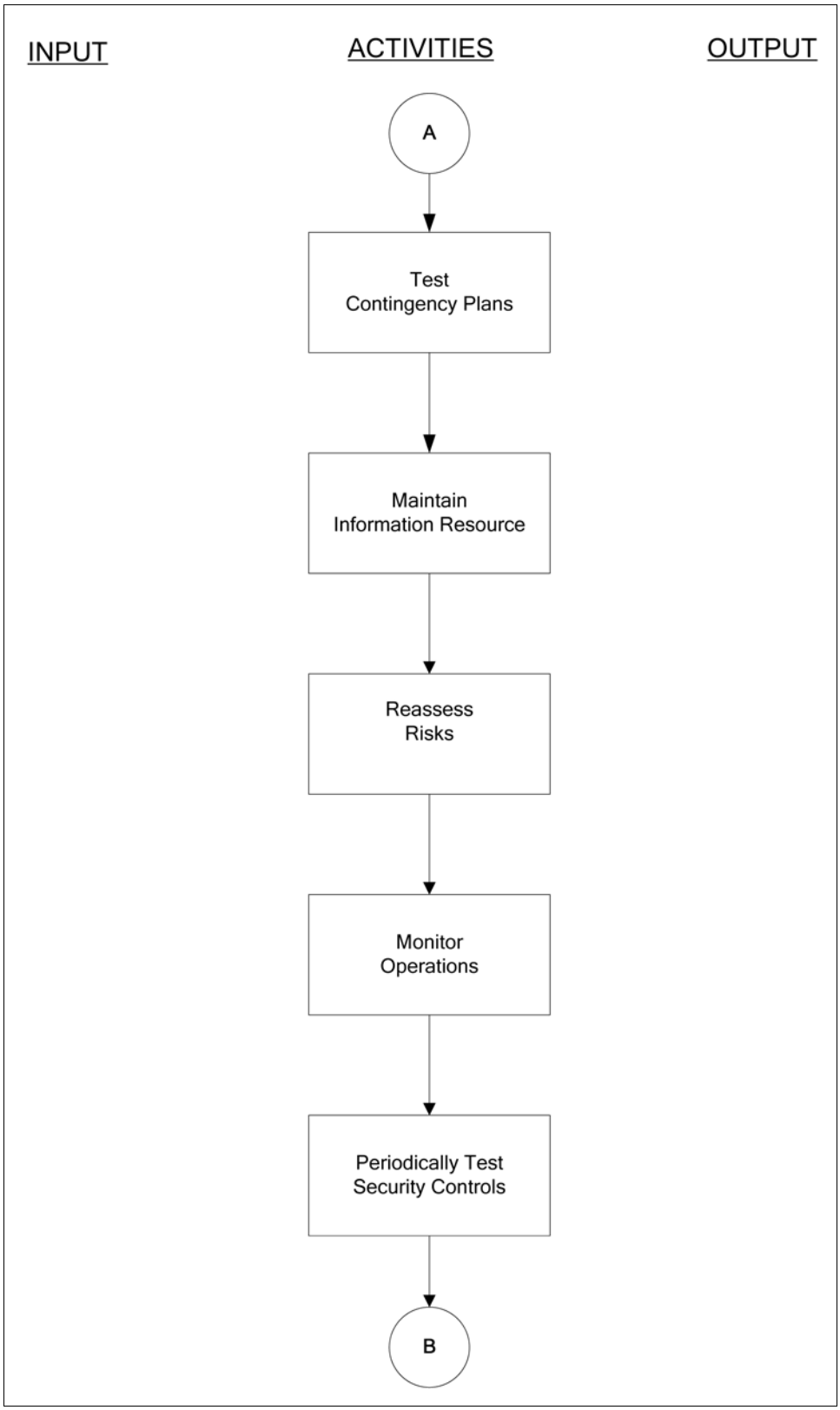


Exhibit 4-7
**Phase 7 Release and Production, (p. 3 of 3)**

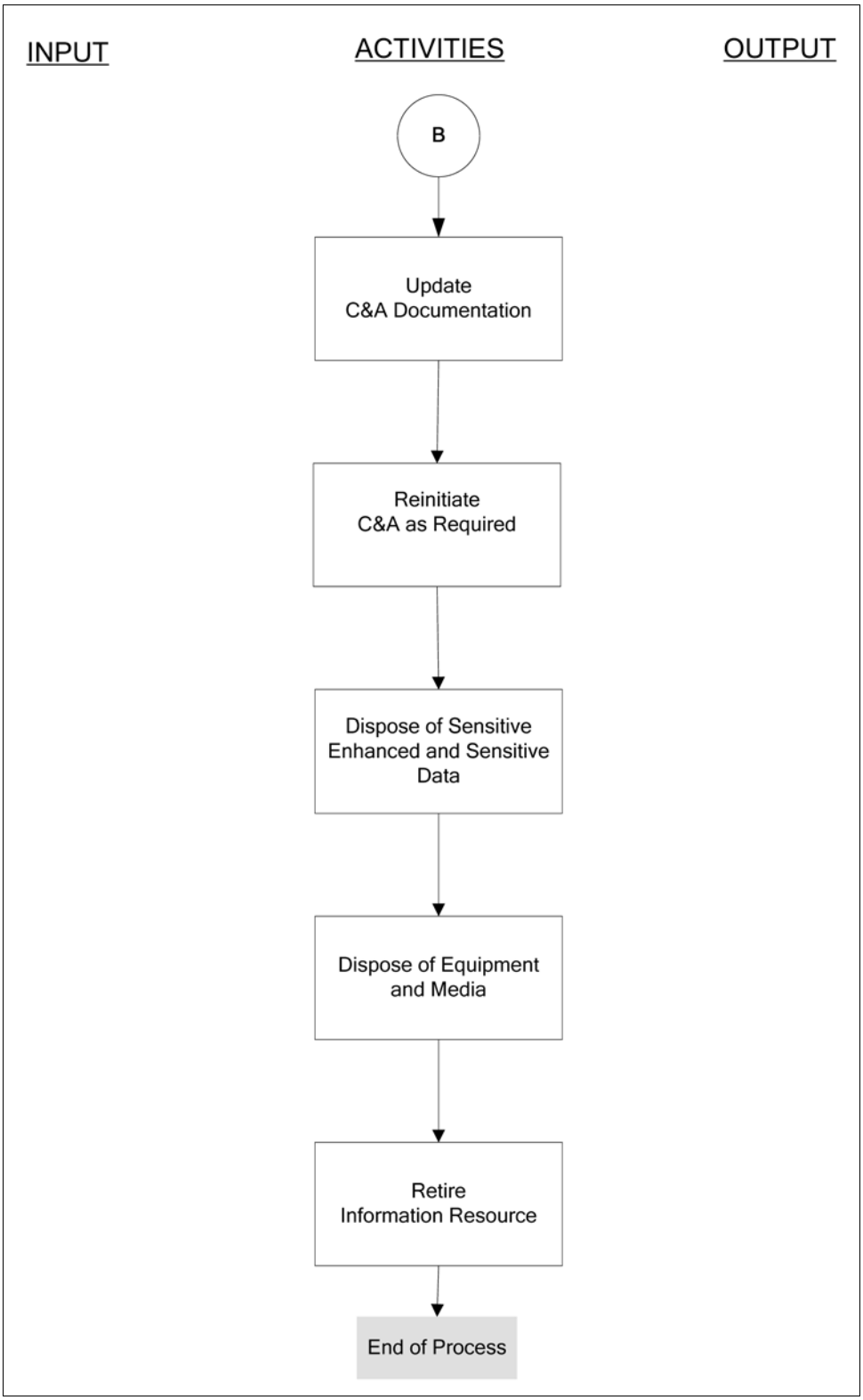


Exhibit 4-7.4.10a
**C&A Templates**

| Template Name | Applicability | Purpose |
|---|---|---|
| Plan of Action and Milestones (POA&M) | For all information resources. | To identify tasks needing to be accomplished with resources required, responsibilities, milestones, and completion dates. Also known as the TSLC Project Plan. |
| Application Characterization | For all information resources. | To provide the background information required to secure the application and Postal Service information. |
| Business Impact Assessment (BIA) | For all information resources. | To determine level of sensitivity and criticality and the information security requirements. |
| Security Plan | For sensitive-enhanced, sensitive, or critical information resources. | To create a blueprint for designing, building, and maintaining an information resource that can be defended against threats and intruders, both internal and external. |
| Risk Assessment | For all information resources. | To identify assets at risk and their value, weaknesses, and vulnerabilities; evaluate threats and vulnerabilities to determine risks; identify additional controls; analyze costs and benefits of the controls; and complete the risk assessment report. |
| Contingency Planning documents | For critical information resources. | To provide cost-effective recovery of an information resource and protection of assets in the event of a significant interruption of computing services. |
| Security Test and Evaluation (ST&E) Plan | For sensitive-enhanced, sensitive, or critical information resources. | To evaluate technical/nontechnical security controls/ safeguards to establish extent to which an information resource meets security requirements. |
| Independent Risk Assessment Report | May be recommended if information resource is publicly accessible; developed, hosted, managed primarily by non-Postal Service personnel; highly visible; or has a high impact. May be required at any time by the CIO; VP IT Solutions; Mgr., CISO; or VP of the functional business area. | To provide a standard report format to document results of independent risk assessment, i.e., one conducted by an entity outside the development organization. |
| C&A Evaluation Report | For sensitive-enhanced, sensitive, or critical information resources. | To document the ISSO's evaluation of technical and nontechnical security features and other safeguards to establish extent to which an information resource meets security requirements. |
| Certification Letter | For sensitive-enhanced, sensitive, or critical information resources. | For the certifier to recommend approval for an information resource to be deployed if the "High" and "Medium" residual risks are mitigated. |
| Risk Mitigation Plan | For sensitive-enhanced, sensitive, or critical information resources where residual risk is "High" or "Medium." | For the portfolio manager to describe the plan to mitigate the "High" or "Medium" residual risks. |
| Acceptance of Responsibility Letter for Documented Vulnerability | For all information resources to document a vulnerability that will not be mitigated. | For the portfolio manager to accept responsibility for a documented vulnerability that will not be mitigated. |

Exhibit 4-7.4.10b

**C&A Requirements for Information Resources**

| | | New & Major Information Resource Modifications | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | NS & NC | | All Other Information Resources | | Recertifications[1] | | Service Based Contracts | |
| **Phase** | **C&A Deliverable** | **Deliverables** | **Responsible** | **Deliverables** | **Responsible** | **Deliverables** | **Responsible** | **Deliverables** | **Responsible** |
| 2. | Application Characterization | Yes | Project Mgr | Yes | Project Mgr | Yes | Project Mgr | Yes | Project Mgr |
| 2 | BIA | Yes | Project Mgr | Yes | Project Mgr | Yes | Project Mgr | Yes | Project Mgr |
| 3 | Security Specs | Yes | Project Mgr | Yes | Project Mgr | If applicable | Project Mgr | Yes | Project Mgr |
| 3 | Security Plan | | | Yes | Project Mgr | If applicable | Project Mgr | Yes | Project Mgr |
| 3 | Risk Assessment | Yes | Project Mgr | Yes | Project Mgr | Yes | Project Mgr | Yes | Project Mgr |
| 3 | Site Security Review | | | Yes | ISSO & USPIS | If applicable | ISSO & USPIS | Yes | ISSO & USPIS |
| 4 | SOPs | | | Yes | Project Mgr | If applicable | Project Mgr | Yes | Project Mgr |
| 4 | Operation Training Matrls | | | Yes | Project Mgr | If applicable | Project Mgr | Yes | Project Mgr |
| 4-5 | Contingency Plans | | | Yes | Project Mgr | If applicable | Project Mgr | Yes | Project Mgr |
| 4 | NCRB Request | Yes | Project Mgr | Yes | Project Mgr | If applicable | Project Mgr | Yes | Project Mgr |
| 5 | ST&E Plan | | | Yes | Project Mgr | If applicable | Project Mgr | Yes | Project Mgr |
| 6 | Security Code Review | Based on Requirements | Project Mgr | Based on Policy Requirements | Project Mgr | If applicable | Project Mgr | Based on Policy Requirements | Project Mgr |
| 6 | ST&E Testing & Report | | | Yes | Project Mgr | If applicable | Project Mgr | Yes | Project Mgr |
| 6 | Vulnerability Scan** | Yes | CISO | Yes | CISO | Yes | CISO | Yes for Sensitive | CISO |
| 6 | Independent Reviews | | | If applicable | Project Mgr | If applicable | Project Mgr | If applicable | Project Mgr |
| 6 | Outstanding Items | | | If applicable | Project Mgr | If applicable | Project Mgr | If applicable | Project Mgr |
| 6 | Evaluation Report | YES | ISSO | Yes | ISSO | Yes | ISSO | | |
| 6 | Certification Letter | YES | ISSO Mgr | Yes | Certifier | Yes | Certifier | | |
| 6 | Risk Mitigation Plan | Yes for High/ Mod Risk | Project Mgr | Yes for High/ Moderate Risk | Project Mgr | Yes for High/ Mod Risk | Project Mgr | Yes for High/ Mod Risk | ISSO |

Exhibit 4-7.4.10b
**C&A Requirements for Information Resources**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 6 | Acceptance of Responsibility for a Vulnerability Letter | Yes for vulnerability that will not be mitigated | Executive Sponsor | Yes for vulnerability that will not be mitigated | Executive Sponsor | Yes for vulnerability that will not be mitigated | Executive Sponsor | Yes for vulnerability that will not be mitigated | Executive Sponsor |
| 6 | Accreditation Letter | YES | Mgr CISO | Yes | Mgr CISO | Yes | Mgr CISO | | |
| 7 | Deployment (Acceptance) Letter | YES | Portfolio Mgr & Executive Sponsor | Yes | Portfolio Mgr & Executive Sponsor | Yes | Portfolio Mgr & Executive Sponsor | Yes | Portfolio Mgr & Executive Sponsor |
| 7 | Contingency Test Results | | | Yes | Portfolio Mgr & Executive Sponsor | Yes | Portfolio Mgr & Executive Sponsor | Yes | Portfolio Mgr & Executive Sponsor |
| 7 | Revised C&A Documents | As needed or every 5 years | ISSO & Project Mgr | As needed or every 3 years; yearly for PCI | ISSO & Project Mgr | As needed or every 3 years; yearly for PCI | ISSO & Project Mgr | As needed or every 3 years | ISSO & Project Mgr |

*Note 1: If the either the BIA and/or Risk Analysis review find major changes have occurred, then follow the New & Major Information Resource Modification process.*

# 5 Independent Reviews

Independent reviews are evaluations conducted by personnel, contractors, or vendors, separate and distinct from the executive sponsor and developers of the information resource, for the purpose of applying rigorous evaluation standards to the information resource. These reviews may be conducted in house or by external contractors.

## 5-1 Independent Security Code Reviews

Custom programs or COTS information resource that contain custom programming or scripts are subject to an independent security code review of the source code and documentation to do the following:

a. Verify compliance with software design documentation and programming standards.

b. Verify the absence of malicious code. (See the manager, Corporate Information Security Information Security Services, for a copy of Information Security Code Review Standards).

c. Evaluate correctness, efficiency, and specific security issues.

These reviews are not substitutes for a standard (rigorously applied) quality assurance process in the development environment.

***Note:*** Unmodified COTS information resources are not subject to an independent security code review.

### 5-1.1 Criteria for Conducting

An independent security code review is recommended by the ISSO during the BIA process for the following information resources:

a. Information resource will be publicly accessible.

b. Information resource transmits information between a Postal Service network and a public or non-Postal Service network, or between a Postal Service demilitarized zone (DMZ) and a public or non-Postal Service network.

c. Sensitive-enhanced, sensitive, or critical information resource will be developed offsite by non-Postal Service personnel.

d. Information resources contains COTS programs containing custom programming (HTML, XML, Java, JavaScript, CGI, ActiveX, etc.) scripts.

***Note:*** An independent security code review may be required at any time

by the CIO, VP IT Solutions; the manager, CISO; or the VP of the functional business area.

### 5-1.2 Definition of COTS

COTS software includes the following types of information resources:

a. Information resources that are sold, leased, and licensed at advertised or negotiated prices.

b. Information resources that contain proprietary code that is usually not released to the buyer.

c. Information resources that are supported and evolved by the vendor, who retains the intellectual property rights.

d. Information resources that are used without modification of the internal code design (but may have modules that can be modified through custom programming by or for the buyer).

***Note:*** The Enterprise Architecture Committee (EAC) determines the acceptability of COTS products for the Postal Service computing environment.

### 5-1.3 Documentation

The person conducting the independent security code review documents the findings and provides the report to the executive sponsor as soon as possible, to allow any deficiencies to be addressed.

## 5-2 Independent Information Security Risk Assessments

Independent information security risk assessments are risk assessments conducted by an organization, office, or contractor that is separate and distinct from the executive sponsor and developers of the information resource. The assessments evaluate the appropriateness and effectiveness of the security controls and identify the residual risk. If an independent risk assessment is required, the risk assessment described in Phase 3 is not required.

### 5-2.1 Criteria for Conducting

An independent risk assessment may be recommended by the ISSO during the BIA process for the following information resources:

a. Information resource will be publicly accessible.

b. Information resource will be developed offsite by non-Postal Service personnel.

c. Information resource will be hosted at a non-Postal Service site.

d. Information resource will be managed primarily by non-Postal Service personnel.

e. Information resource will have high visibility and impact will be high if something negative happens.

***Note:*** An independent risk assessment may be required at any time by

the CIO, VP IT Solutions; the manager, CISO; or the VP of the functional business area.

### 5-2.2 Guidelines

Independent risk assessments may be completed by an in-house organization or an external organization. Independent risk assessments conducted in-house are completed using the Risk Assessment process and templates available on the IT Web site; select TSLC Templates; under the Analysis and Design phase, select Risk Assessment.

External independent risk assessments are completed using the External Information Security Independent Risk Assessment process and templates (See the manager, Corporate Information Security Information Security Services, for a copy of External Independent Risk Assessment).

The external independent risk assessment includes the following activities:

a. Identifying the assets that comprise the information resource.

b. Analyzing the probability and impact of threats.

c. Analyzing the vulnerabilities that could increase the probability or impact of threats.

d. Analyzing the appropriate countermeasures for identified threats and vulnerabilities.

e. Identifying residual risk after the installation of security controls.

f. Determining if the risk will be accepted, transferred, or further mitigated.

g. Summarizing the risk status of the information resource.

### 5-2.3 Documentation

The person conducting the independent risk assessment documents the findings and provides the report to the executive sponsor as soon as possible, to allow any deficiencies to be addressed.

## 5-3 Independent Vulnerability Scans

Independent vulnerability scans evaluate the effectiveness of the implemented configuration and security settings. These tests scan information resources for vulnerabilities and compliance with Postal Service information security policies and standards.

### 5-3.1 Criteria for Conducting

Independent vulnerability scans are required as follows:

a. New sensitive-enhanced, sensitive, or critical information resources.

b. Quarterly for internal and external PCI scans.

c. Annually for publicly accessible (externally facing) information resources.

d. Information resource with access to or communication through a public or non-Postal Service network.

e. Information resources developed, hosted, or managed primarily by non-Postal Service personnel.

***Note:*** Independent vulnerability scans may be required at any time by the CIO, VP IT Solutions; manager, CISO; or the VP of the functional business area.

### 5-3.2 Documentation

The person conducting the vulnerability scans documents the findings and provides the report to the executive sponsor as soon as possible, to allow any deficiencies to be addressed.

## 5-4 Independent Penetration Testing

Independent penetration testing evaluates the effectiveness of the implemented configuration and security settings.

### 5-4.1 Criteria for Conducting

Independent penetration testing may be recommended by the ISSO during the BIA process for the following information resources:

a. Sensitive-enhanced, sensitive, or critical information resources.

b. Publicly accessible (externally facing) information resources.

c. Information resource with access to or communication through a public or non-Postal Service network.

d. Information resources developed, hosted, or managed primarily by non-Postal Service personnel.

***Note:*** Independent penetration testing may be required at any time by the CIO, VP IT Solutions; manager, CISO; or the VP of the functional business area.

### 5-4.2 Documentation

The person conducting the penetration testing documents the findings and provides the report to the executive sponsor as soon as possible, to allow any deficiencies to be addressed.

## 5-5 Independent Security Test Validation

The independent security test validates the appropriateness and effectiveness of the security controls implemented for information resources and corroborates the previously conducted ST&E test results.

## 5-5.1 Scope

The scope of the independent security test validation depends on the information resource, its environment, and the associated threats and vulnerabilities. The security test validation is usually carried out at the development or test site.

## 5-5.2 Criteria for Conducting

An independent security test validation may be recommended by the ISSO during the BIA process for the following information resources:

a. Information resource will be publicly accessible.

b. Information resource transmits information between a Postal Service network and a public or other non-Postal Service network, or between a Postal Service DMZ and a public network or non-Postal Service network.

c. Information resource will be developed offsite by non-Postal Service personnel.

d. Information resource will be hosted at a non-Postal Service site.

e. Information resource will be managed primarily by non-Postal Service personnel.

***Note:*** An independent security test validation may be required at any time by the CIO, VP IT Solutions; the manager, CISO; or the VP of the functional business area.

## 5-5.3 Process

The independent security test validation process is generally conducted through the following steps:

a. At the beginning of Phase 3, the person conducting the validation defines the security test plan criteria for independent testing and may confer with the portfolio manager, executive sponsor, project manager, developers, ISSO, and subject-matter experts as required.

b. During Phase 3, a date is set for the security test validation, providing at least a 1-week lead time to the project manager, developers, contractor, or business partner. The setting of test dates is based on discussions with the executive sponsor and the project manager, developers, contractor, or business partner.

c. The day before the validation is conducted, the security test validation criteria are provided to the development team. This allows the development team to plan on having the necessary personnel available for conducting the tests.

## 5-5.4 Documentation

After conducting the independent security test validation, the person conducting the validation documents the findings and provides the report to the executive sponsor as soon as possible, to allow any deficiencies to be addressed.

This page intentionally left blank

# 6 Re-Initiating the Certification and Accreditation

## 6-1 Purpose

The purpose of re-initiating the C&A (Re-C&A) is to ensure that the following conditions are met:

a. Existing security controls and processes for the information resource are still in place and functioning correctly.

b. Changes to the information resource requiring new or modified security controls and processes are properly addressed.

c. Security controls, processes, and responsibilities are still appropriate based on organizational changes within the Postal Service.

d. Security controls and processes are still appropriate based on the discovery of new vulnerabilities or how new technologies impact those controls.

## 6-2 Criteria Forcing Security Recertification

Scheduled recertification is required every 1 year for PCI designated information resources; every 3 years for sensitive-enhanced, sensitive, or critical information resources; and every 5 years for nonsensitive or noncritical information resources.

Unscheduled recertification is required if the specific information resources changes meet one or more of the following criteria:

a. Changes to the information resources that alter the information resource's criticality or sensitivity designation.

b. The addition of new data element(s) that alter the information resource’s sensitivity designation.

c. Rewriting the application or the addition or modification of entry points of an information resource.

d. Major database version changes (i.e., ORACLE 9 to ORACLE 10.) Minor releases, which are designated by sub number or letter (i.e., ORACLE 9.1 to ORACLE 9.2), do not require Recertification. If a database is certified as an infrastructure, then only the database would need to be recertified and not all the applications using it.

e. Changing from one database system to another, (i.e., Oracle to MS-SQL.) If the new database is certified as an infrastructure, then the application would not require a recertification.

f. Changing the hosting location (i.e., Postal Service glass house location to an outsourced/non-Postal Service location or a Postal Service non-glass house location.)

g. Any code changes to the application code of an outwardly-facing application. Changes to the content of a content driven application will not require a Recertification.

h. Newly discovered vulnerabilities or threats that alter the risk to an application.

i. Changing the operating environment in which the application runs on (e.g., Windows XP to UNIX, UNIX to LINUX, Windows NT to Windows XP, Windows XP to Windows Vista). Adding additional hardware (e.g., servers) without making any changes to the application or infrastructure is not considered a change in the operating environment.

j. An application that has had an information security incident that violates a security/privacy policy and compromised the integrity, availability, or confidentiality of its data (e.g., a critical disruption in service, a monetary loss, the unauthorized modification of sensitive or critical information, the release of sensitive or critical information).

k. Modifications to an inwardly-facing application that makes it outwardly-facing or moving the application from an enclave or into a DMZ.

A request by the CIO or designee; VP IT Solutions; the manager, CISO; the VP of the functional business area; or the executive sponsor based upon an audit finding or possibility of a vulnerability whose presence must be dispelled or validated.

# 6-3 Process

## 6-3.1 Requesting a Re-C&A

At the appropriate time or other reason documented above, the executive sponsor addresses a letter to the manager, CISO, requesting a Re-C&A. The letter should provide details specific to the information resource and the reason for the Re-C&A.

## 6-3.2 Conducting a Re-C&A

The security deliverables from each of the Phases of the latest C&A process should be reviewed, updated as required, signed, and dated. The Re-C&A follows the normal C&A process.