UNITED STATES
POSTAL SERVICE®

Infrastructure Information Security Assurance (ISA) Process

Handbook AS-805-B

March 2005
Transmittal Letter

A. Explanation. As part of the Postal Service's efforts to enhance security across all technology in accordance with its Transformation Plan, this handbook establishes the process and guidance for the Postal Service information security assurance for major information technology (IT) infrastructure components. The process provides a framework for defining security requirements and controls, assessing risk, testing security solutions, and evaluating the security posture of Postal Service IT infrastructure to ensure that appropriate, cost-effective information security controls and processes are implemented.

B. Distribution. This document is available on the Postal Service Intranet at *http://blue/cpim/hbkid.*

C. Comments and Questions. Submit comments and questions to:

CORPORATE INFORMATION SECURITY OFFICE
UNITED STATES POSTAL SERVICE
4200 WAKE FOREST ROAD
RALEIGH NC 27668-1510

Comments may also be sent by e-mail to *information_security@usps.gov.* Use "AS-805-B Infrastructure ISA Process" in the subject header.

D. Effective Date. This handbook is effective immediately.

Robert L. Otto

Robert L. Otto
Vice President, Chief Technology Officer

Contents

Exhibits

1 Introduction

1-1 About This Handbook

This handbook contains a high-level description of the Postal Service infrastructure information security assurance (ISA) process, identifies the roles and responsibilities, and provides pointers to instructions and templates to complete each phase of the process.

1-2 Purpose of Infrastructure ISA

Infrastructure ISA is the process the Postal Service uses to evaluate the protection of its infrastructure components so that risks associated with deployment can be appropriately managed throughout the life cycle of the infrastructure components.

1-3 Importance of Infrastructure ISA

Infrastructure — The underlying base or foundation for information resources including physical and cyber-based resources (i.e., facilities, network hardware and software, and environmental support services). The infrastructure components addressed in this handbook are major groupings or network segments that provide reusable and repeatable services for application systems.

This process provides Postal Service infrastructure owners with a consistent method for making informed decisions on managing security risks related to their infrastructure. Benefits include the following:

a. Protection of the integrity of the Postal Service brand.

b. A structured view of the potential risks associated with infrastructure and the relationships among business partnerships.

c. Documented implementation of information security controls and processes that protect Postal Service infrastructure.

d. A secure platform to build protection measures for the confidentiality, integrity, and availability of Postal Service information resources.

e. A secure platform to build protection measures for the privacy of employees and customers.

f. Protection of Postal Service assets.

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

1-4 General Infrastructure Observations

Security — The condition achieved when designated information, equipment, personnel, processes, and facilities are protected against threats. Privacy is a key component of security.

Privacy — The protection afforded individuals from the collection, storage, and dissemination of information about themselves and possible compromises resulting from unauthorized release of that information.

Infrastructure components are generally considered to be critical components of the Postal Service computing environment. Infrastructure components must generally be capable of processing sensitive information and applications.

2 Roles and Responsibilities

This chapter defines the roles and responsibilities for the infrastructure ISA process.

2-1 Chief Inspector

Certification — The technical analysis that establishes the extent to which an application meets specified security requirements.

The chief inspector is responsible for providing physical security as well as personnel clearance consultation and guidance during infrastructure implementation to assure that security concerns are addressed and that information and/or evidence that may be needed for an investigation is retained by the infrastructure owner.

2-2 Manager, Corporate Information Security Office

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

a. Developing and maintaining the infrastructure ISA process.

b. Managing the CISO support for the infrastructure ISA process.

c. Appointing information systems security officers (ISSOs).

d. Reviewing the infrastructure ISA documentation package and escalating security concerns or accrediting the infrastructure component.

2-3 Executive Sponsors

IIA — The process to identify the appropriate information security requirements to protect the infrastructure component based on the sensitivity and criticality of the hosted applications.

Executive sponsors are responsible for the following:

a. Ensuring the completion of all security-related tasks throughout the life cycle of an infrastructure component.

b. Funding information security controls that satisfy the information security requirements and the documentation requirements associated with the infrastructure ISA process for infrastructure components under their purview.

c. Implementing security controls that satisfy the security requirements defined in the infrastructure impact assessment (IIA).

d. Accepting any residual risk associated with deployment of the infrastructure component.

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

2-4 Program Managers

Program managers for the infrastructure component development, acquisition, or integration are responsible for the following:

a. Managing the development and implementation efforts for new infrastructure components, whether developed in-house, outsourced, or acquired.

b. Incorporating the appropriate security controls in all infrastructure components, whether developed in-house, outsourced, or acquired, to satisfy the security requirements defined in the IIA.

c. Completing the required infrastructure ISA documentation including high-level architectural diagram, security specifications, standard operating procedures, security plan, security test and evaluation plan, and security test and evaluation report.

2-5 Accreditor

The manager, Corporate Information Security Office, functions as the accreditor and is responsible for the following:

a. Reviewing the risk mitigation plan and supporting infrastructure ISA 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 infrastructure component 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 infrastructure ISA documentation package to the executive sponsor.

2-6 Certifier

The manager, Information Security Assurance, functions as the certifier and is responsible for the following:

a. Managing and providing guidance to the information systems security officers (ISSOs).

b. Reviewing the infrastructure ISA evaluation report and the supporting infrastructure ISA documentation package.

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

d. Forwarding the certification letter and infrastructure ISA documentation package to the accreditor.

e. Maintaining an inventory of all infrastructure components that have completed the infrastructure ISA process.

2-7 Information Systems Security Officers

Information systems security officers (ISSOs) are responsible for the following:

a. Providing information security and infrastructure ISA guidance.

b. Completing the IIA.

c. Coordinating the completion of the infrastructure risk assessment.

d. Reviewing the infrastructure ISA documentation and any independent reviews of the infrastructure components.

e. Preparing the infrastructure ISA evaluation report.

f. Forwarding the infrastructure ISA documentation package to the certifier.

2-8 Contracting Officers

Contracting officers are responsible for the following:

a. Ensuring that information technology contractors, vendors, and business partners are contractually obligated to abide by information security policies, standards, and procedures, including the infrastructure ISA.

b. Ensuring that the security requirements are specified in the contractual agreements.

2-9 Business Partners

Business partners developing or hosting infrastructure components for the Postal Service are responsible for the following:

a. Abiding by Postal Service information security policies, regardless of where the infrastructure components 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 contract representatives.

This page intentionally left blank

3 Overview of Infrastructure ISA

3-1 What The Infrastructure ISA Consists Of

The infrastructure ISA process consists of the following five interrelated phases that are conducted concurrently with the development and deployment of new infrastructure components (i.e., during the Integrated Solutions Methodology (ISM) System Development Lifecycle (SDLC):

- Phase 1 — Definition.
- Phase 2 — Design and Integration.
- Phase 3 — Testing.
- Phase 4 — Evaluation.
- Phase 5 — Production.

The infrastructure ISA process, located in Exhibit 3-1, documents the *sensitivity* and *criticality* of the hosted Postal Service applications, defines information security requirements, determines appropriate security controls and processes to satisfy the security and privacy requirements, tests the effectiveness of implemented security controls and processes, evaluates the threats and vulnerabilities associated with the infrastructure components and the risks associated with deployment, and culminates with certification. During the production phase, the infrastructure component is maintained with the appropriate security to manage the residual risk. The infrastructure ISA process is repeated every 3 years or as required to ensure the continuing security of the infrastructure component (see Chapter 5).

ISM-SDLC — The procedures, practices, and guidelines governing the initiation, concept development, planning requirements analysis, design, development, integration and test, implementation, operations, maintenance, and disposition of information resources in the Postal Service system.

Sensitivity — The degree to which the Postal Service must protect the confidentiality and integrity of information. Levels of sensitivity are *sensitive, business-controlled sensitivity, and nonsensitive.*

3-2 What the Infrastructure ISA Applies To

The infrastructure ISA process applies to all infrastructure components 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 infrastructure ISA also applies to pilot and proof-of-concept projects.

Criticality — The degree to which the Postal Service must provide for continuous availability of information. Levels of criticality are *critical, business-controlled criticality, and noncritical.*

3-3 Infrastructure ISA Phases, Activities, and Deliverables

Exhibit 3-1 depicts the five infrastructure ISA phases and the major activities and deliverables required during each phase.

3-4 Frequency of the Infrastructure ISA

Certification — The technical analysis that establishes the extent to which an application meets specified security requirements.

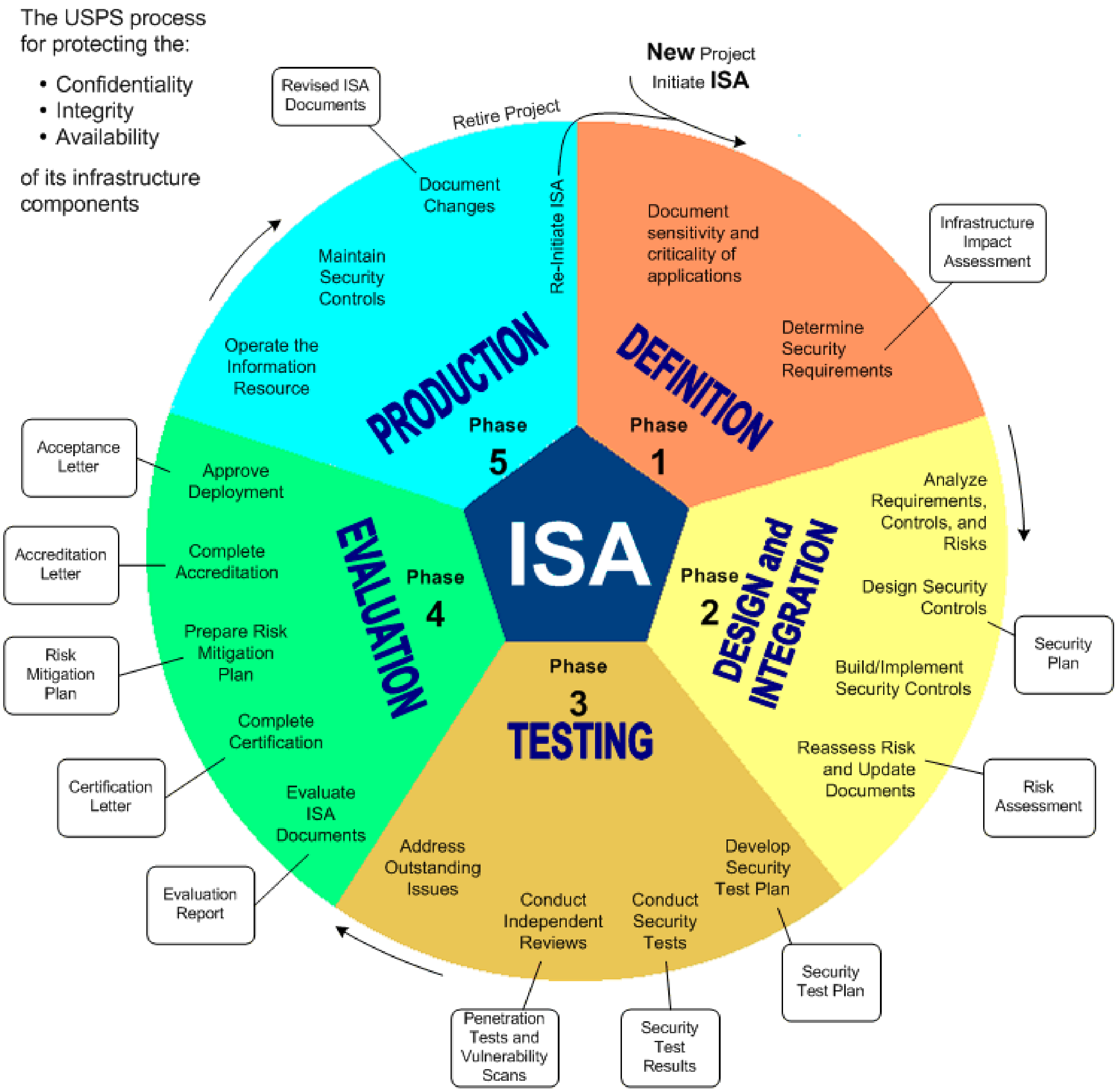
The infrastructure ISA is performed at least every 3 years on an infrastructure component following its last certification or sooner if the infrastructure component undergoes significant change. See Chapter 5, Re-Initiating the Infrastructure ISA, for specific reasons.

3-5 Funding of the Infrastructure ISA

Significant change — A change that calls into question the security of an information resource and the accuracy of previous infrastructure ISA documentation.

Funding for the infrastructure ISA 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 infrastructure ISA process.

Exhibit 3-1
Infrastructure ISA Phases and Major Deliverables



This page intentionally left blank

4 The Infrastructure ISA Process

This chapter describes each phase in the infrastructure ISA process. At the end of this chapter, Exhibit 4a provides a list of infrastructure ISA guidelines, templates, and related Web links.

4-1 Phase 1 – Definition

Phase 1 applies to infrastructure components 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 new business partner initiatives. It begins when the manager CISO or the executive sponsor requests the initiation of the infrastructure ISA process. (See Exhibit 4-1, Phase 1.)

4-1.1 Objectives

Phase 1 objectives are as follows:

a. Documenting the sensitivity and criticality of the applications hosted on the infrastructure component.

b. Developing a high-level architecture diagram.

c. Identifying connectivity requirements.

d. Determining security requirements to mitigate risk based on the sensitivity, criticality, and the business needs of the Postal Service.

4-1.2 Deliverables

The deliverables for Phase 1 are the following:

a. A high-level architectural diagram.

b. A completed IIA.

c. The security requirements incorporated in the service level agreement (SLA) and trading partner agreement (TPA), if applicable.

4-1.3 Roles and Responsibilities

Roles	Responsibilities
Executive sponsor	Ensures completion of Phase 1 activities.
Program manager	Develops a high-level architectural diagram. Develops SLA and TPA if applicable.
ISSO	Provides guidance and consulting support. Coordinates the completion of the IIA.

4-1.4 Activities

4-1.4.1 Hold Infrastructure ISA Meeting

The ISSO assigned to the infrastructure component holds an infrastructure ISA meeting to discuss the proposed infrastructure component and its business requirements and the infrastructure ISA process. ISSOs are encouraged to pursue flexible and cost-effective communication approaches, such as teleconferencing or videoconferencing.

4-1.4.2 Review Documentation

The ISSO reviews applicable infrastructure documentation. Some of the documentation could include the following:

a. Original business needs statement, business case, request for proposal, and statement of work.

b. SLAs, contracts, and project plans.

c. Policies, procedures, and any other applicable documentation that may affect the infrastructure component.

4-1.4.3 Develop High-Level Architectural Diagram

A high-level architectural diagram (e.g., hardware, communications, security devices, and interconnected resources) must be developed and submitted to the manager, Secure Infrastructure Services, for review and determination of the impact on the Postal Service infrastructure and the need for additional network security controls.

4-1.4.4 Complete Infrastructure Requirements Determination

An IIA must be completed which includes the following steps:

a. Documenting the sensitivity and criticality of the applications hosted on the infrastructure component.

b. Engaging the Network Connectivity Review Board if necessary.

c. Determining the information security requirements.

4-1.4.5 Incorporate Information Security Requirements in SLAs and TPAs

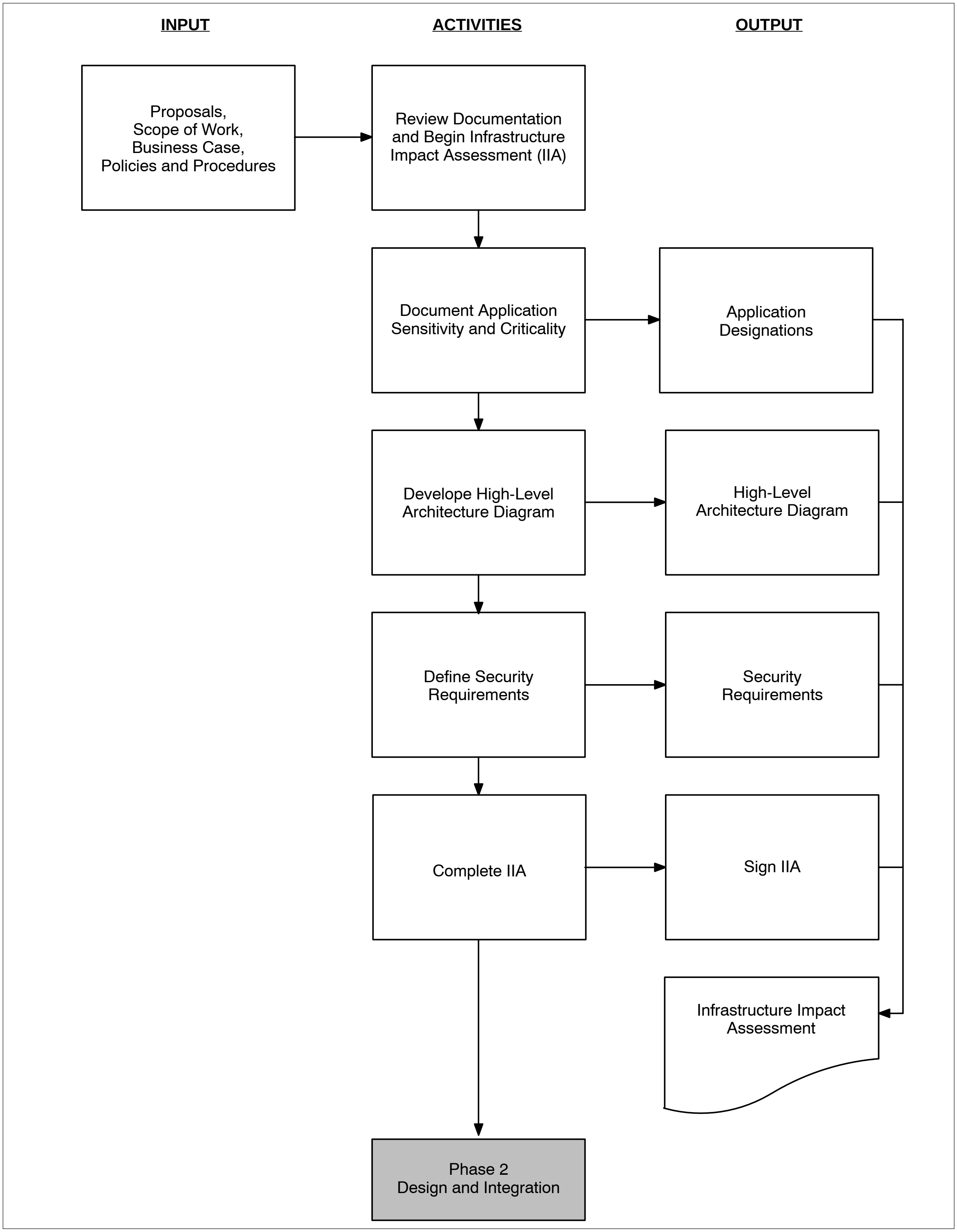
Information security requirements must be incorporated in SLAs and TPAs, if applicable. An SLA is developed for all infrastructure components, and a TPA is developed for all externally managed or developed infrastructure components.

4-1.4.6 Update Project Plan

Once the IIA is completed, the Program Manager ensures that the project plan is revised to include integrating information security controls in the infrastructure component and the deliverables associated with the infrastructure ISA process.

Exhibit 4-1

Phase 1, Definition


INPUT
ACTIVITIES
OUTPUT
Proposals, Scope of Work, Business Case, Policies and Procedures
Review Documentation and Begin Infrastructure Impact Assessment (IIA)
Document Application Sensitivity and Criticality
Application Designations
Develope High-Level Architecture Diagram
High-Level Architecture Diagram
Define Security Requirements
Security Requirements
Complete IIA
Sign IIA
Infrastructure Impact Assessment
Phase 2 Design and Integration

4-2 Phase 2 – Design and Integration

Phase 2 identifies security controls and processes which will satisfy the security requirements defined during Phase 1. (See Exhibit 4-2, Phase 2.)

4-2.1 Objectives

Phase 2 objectives are as follows:

a. Identifying security controls and processes for security requirements defined during Phase 1.

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

c. Identifying the risks associated with the infrastructure component.

4-2.2 Deliverables

The deliverables for this phase are the following:

a. Infrastructure risk assessment.

b. Security specifications.

c. Infrastructure security plan.

d. Standard operating procedures.

4-2.3 Roles and Responsibilities

Roles	Responsibilities
Executive sponsor	Ensures completion of Phase 2 activities.
Program manager	Develops infrastructure security specifications, standard operating procedures, and security plan.
ISSO	Provides guidance and consulting support. Coordinates the completion of the infrastructure risk assessment.

Note: If the projected dates of delivery of the deliverables change, the project plan should be amended and the ISSO should be notified of the changes.

4-2.4 Activities

4-2.4.1 Analyze Requirements and Identify Potential Security Controls

Analyze security requirements established for the infrastructure and identify potential security controls in light of business requirements, Postal Service policies, and cost versus benefit of the various control options.

4-2.4.2 Assess Risks

Risks depend on the configuration of the infrastructure and the implementation environment. An infrastructure risk assessment must be completed.

4-2.4.2.1 Infrastructure Risk Assessment

The infrastructure risk assessment is an ongoing process designed to minimize risk to infrastructure components 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 those assets.

4-2.4.2.1.1 Infrastructure Risk Assessment Activities

An infrastructure risk assessment will do the following:

a. Identify general administrative data and assets.

b. Identify possible threats that could adversely affect the infrastructure.

c. Identify security vulnerabilities that could be exploited by threat events affecting the infrastructure.

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 infrastructure.

h. Identify possible additional mitigating controls that, if applied, could be expected to mitigate the risks identified for the infrastructure.

i. Document the overall risk status of the infrastructure.

4-2.4.2.1.2 Infrastructure Risk Assessment Roles and Responsibilities

Roles	Responsibilities
Executive sponsor	Ensures completion of infrastructure risk assessment for infrastructure components under their purview. Provides personnel and financial resources to support risk assessment activities. Accepts any residual risk associated with infrastructure.
Program manager	Works with the ISSO to complete the risk assessment.
ISSO	Provides guidance on applicability of threats or vulnerabilities and appropriate choice of countermeasures. Coordinates the completion of the risk assessment.

4-2.4.3 Select/Design Security Controls

4-2.4.3.1 General

Security controls must be selected to satisfy the security requirements identified in the IIA during Phase 1 and to mitigate the risks identified in the infrastructure risk assessment. 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.

4-2.4.3.2 Selecting Security Controls

Information security controls are selected based on their capability to be implemented in the infrastructure, a cost-benefit analysis of the controls, business needs, and compatibility with other Postal Service security controls and processes. Circumstances peculiar to the infrastructure, changes in technologies, and the discovery of new vulnerabilities in what had been considered “safe” products may lead to additional security controls.

4-2.4.4 Document Security Specifications

The security specifications must be documented for use in the acquisition of information security products and services or their development.

4-2.4.5 Acquire, Build, and Integrate Information Security Controls

The development team acquires, builds, and integrates the information security controls and processes and keeps the ISSO informed of their progress.

4-2.4.6 Develop Infrastructure Security Plan

4-2.4.6.1 General

An infrastructure security plan must be developed. The security plan is a blueprint for protecting the infrastructure component in the production environment. It 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 application.

4-2.4.6.2 Infrastructure Security Plan Roles and Responsibilities

Roles	Responsibilities
Executive sponsor	Provides personnel and financial resources to support development of an infrastructure security plan.
Program manager	Completes the infrastructure security plan.
ISSO	Provides guidance and consulting support.
Development team	Implements specific security controls and processes and keeps Program Manager and ISSO informed of progress.

4-2.4.7 Harden Information Resources

The infrastructure 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.

4-2.4.8 Develop Standard Operating Procedures

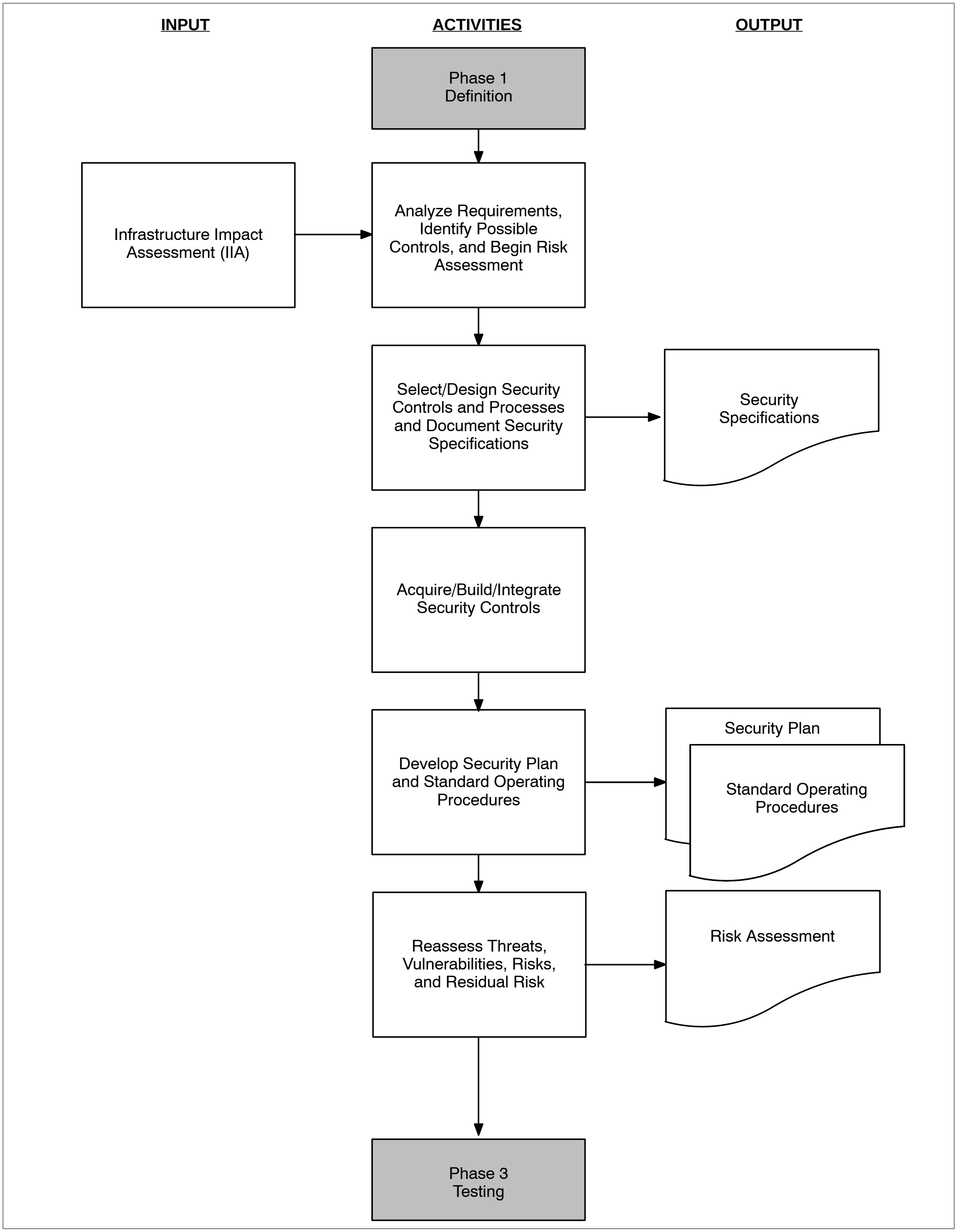
Standard operating procedures must be developed to handle the operating support required for the infrastructure. These procedures cover such topics as separation of duties, manual processes, and report distribution.

4-2.4.9 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 computing 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 infrastructure. The infrastructure risk assessment should be updated as required.

Exhibit 4-2

Phase 2, Design and Integration


INPUT
ACTIVITIES
OUTPUT
Phase 1 Definition
Infrastructure Impact Assessment (IIA)
Analyze Requirements, Identify Possible Controls, and Begin Risk Assessment
Select/Design Security Controls and Processes and Document Security Specifications
Security Specifications
Acquire/Build/Integrate Security Controls
Develop Security Plan and Standard Operating Procedures
Security Plan
Standard Operating Procedures
Reassess Threats, Vulnerabilities, Risks, and Residual Risk
Risk Assessment
Phase 3 Testing

4-3 Phase 3 – Testing

Phase 3 focuses on testing the security controls and processes defined in the infrastructure security plan and implemented in Phase 2 to determine their effectiveness.

4-3.1 Objectives

Determine effectiveness of security controls and processes defined in the infrastructure security plan and implemented in Phase 2. (See Exhibit 4-3, Phase 3.)

4-3.2 Deliverables

The deliverables in this phase are the following:

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

b. Infrastructure ST&E report.

c. Operational security training.

d. Independent reviews.

4-3.3 Roles and Responsibilities

Roles	Responsibilities
Executive sponsor	Ensures completion of Phase 3 activities.
Program manager	Coordinates the development of the infrastructure security test and evaluation plan. Coordinates the infrastructure security test and evaluation. Coordinates the security test and evaluation report preparation.
ISSO	Provides guidance and consulting support. Participates in security testing when possible. Coordinates any independent reviews.
Development team	Designs test procedures and scripts to test specific security controls and processes. Tests the security controls and processes. Documents test results.

Note: If the projected delivery dates of the infrastructure security test and evaluation plan, infrastructure security test and evaluation report, or independent reviews change, the project plan must be amended and the ISSO notified of the changes.

4-3.4 Activities

4-3.4.1 Develop Infrastructure Security Test and Evaluation Plan

4-3.4.1.1 General

The ST&E plan addresses the security testing to be conducted. If the ST&E plan is part of the overall system test plan, highlight or flag the security section for ease of review.

4-3.4.1.2 Build Infrastructure Security Test and Evaluation Plan

All of the stakeholders should be consulted to determine the process by which the security test and evaluation is conducted.

The infrastructure ST&E plan must:

a. Address the security controls and processes described in the infrastructure security plan and the means by which those controls and processes will be tested.

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

c. Describe the actual testing to be performed for each control. Include applicable test scripts, scenarios, performance thresholds, and an indication of pass or fail for each control.

4-3.4.2 Conduct the Infrastructure Security Test and Evaluation

4-3.4.2.1 Conduct Security Test Process

The security test must be performed in accordance with the infrastructure ST&E plan to reduce the risk of false or faulty test results. If a modification to a control is required, the change should be reflected in the ST&E plan before the test is executed.

4-3.4.2.2 Develop Infrastructure Security Test and Evaluation Report

Upon completion of the testing:

a. The development team documents the test results in an infrastructure ST&E report and submits the findings to the executive sponsor. If the ST&E report is a part of the 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 and program manager, reviews the findings and determines whether the security controls and processes are adequate to protect the infrastructure component or whether modifications to the security controls and processes are warranted. If modifications are warranted, the infrastructure ST&E plan is amended and testing reinitiated.

4-3.4.3 Conduct Operational Security Training

Users, system administrators, management, and other personnel must be trained on the correct use of the infrastructure component and its security safeguards.

4-3.4.4 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 risk assessments.

b. Independent penetration testing and vulnerability scans.

c. Independent security test validations.

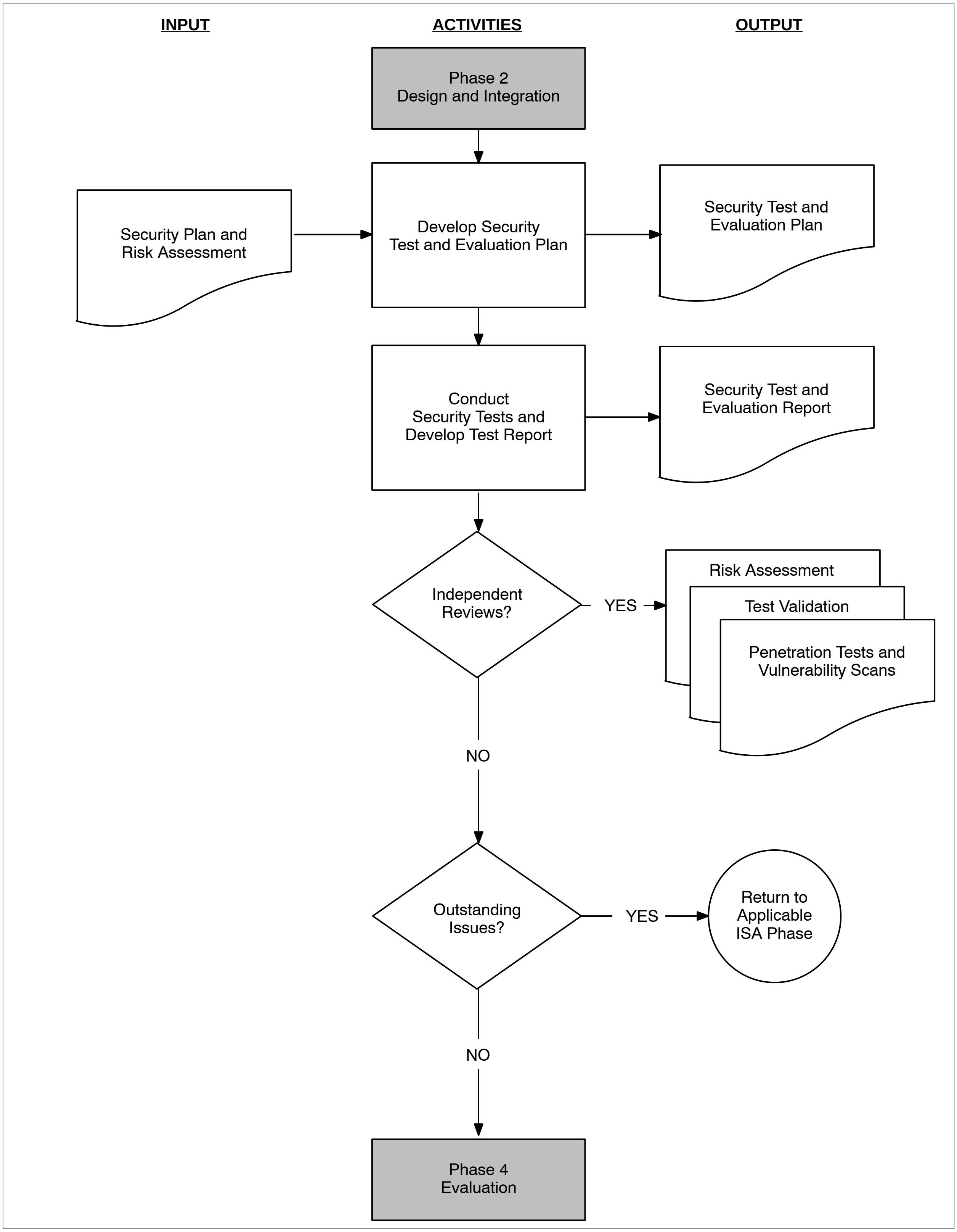
These independent reviews are discussed in Handbook AS-805-A, *Application Information Security Assurance (ISA) Process,* Chapter 5, Independent Reviews.

4-3.4.5 Resolve Outstanding Issues

Any outstanding issues must be resolved and the applicable infrastructure ISA Phase revisited before Phase 4, Evaluation, is initiated.

Exhibit 4-3

Phase 3, Testing



4-4 Phase 4 – Evaluation

Phase 4 consists of those activities that culminate in certification and acceptance of risk of the infrastructure component. (See Exhibit 4-4, Phase 4.)

4-4.1 Objectives

The objectives of this phase are to certify and accept residual risk of the infrastructure component.

4-4.2 Deliverables

The deliverables of this phase are the following:

a. Infrastructure ISA evaluation report.

b. Certification letter.

c. Risk mitigation plan.

d. Accreditation letter.

e. Acceptance letter.

4-4.3 Roles and Responsibilities

Roles	Responsibilities
ISSO	Evaluates infrastructure ISA documentation, prepares an infrastructure ISA evaluation report that details the findings, and forwards the infrastructure ISA documentation package to the certifier.
Certifier	Reviews the infrastructure ISA documentation package, makes the decision to escalate security concerns or prepares and signs a certification letter that summarizes the findings, reviews and updates the infrastructure risk assessment as required, prepares a risk mitigation plan for residual risks rated as medium or high, and forwards the infrastructure ISA documentation package to the accreditor.
Accreditor	Reviews infrastructure ISA documentation package and makes the decision to escalate security concerns or prepares and signs an accreditation letter, and forwards the infrastructure ISA documentation letter to the executive sponsor.
Executive sponsor	Provides personnel and financial resources for correcting deficiencies. Accepts any residual risk associated with deployment.
Other stakeholders	Participate by responding on outstanding issues or providing advisory support.

4-4.4 Activities

4-4.4.1 Evaluate Infrastructure ISA Documentation

The ISSO initiates the evaluation of infrastructure ISA documentation package early in the infrastructure ISA process. This enables the developers to be proactive in identifying and addressing information security concerns. The infrastructure ISA documentation package includes:

a. IIA.

b. Infrastructure security plan and supporting documentation.

c. Infrastructure risk assessment.

d. Infrastructure ST&E plan.

e. Infrastructure ST&E report.

f. Independent reviews, if applicable.

4-4.4.2 Prepare Infrastructure ISA Evaluation Report

Upon completion of the evaluation, the ISSO prepares an infrastructure ISA evaluation report that details the results and forwards the infrastructure ISA documentation package to the certifier for review.

4-4.4.3 Escalate Security Concerns or Certify Infrastructure Component

The certifier escalates security concerns or prepares and signs an infrastructure certification letter summarizing the findings.

4-4.4.4 Prepare Risk Mitigation Plan

The certifier and program manager then review and update the infrastructure risk assessment completed in Phase 2 as required. For any residual risks rated as medium or high, a risk mitigation plan is prepared recommending whether the risks should be accepted, transferred, or further mitigated. The certifier forwards the infrastructure ISA documentation package to the accreditor for review.

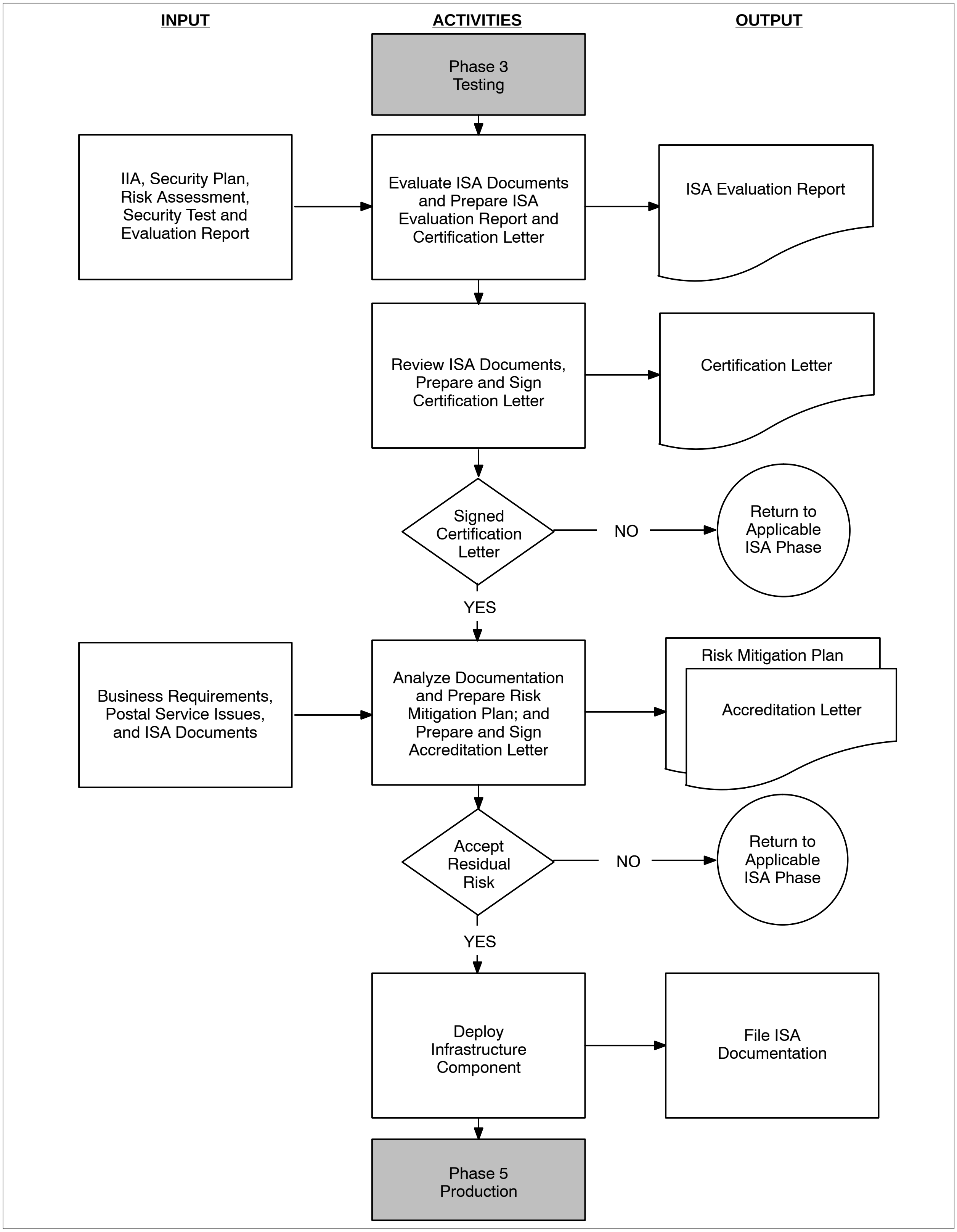
4-4.4.5 Escalate Security Concerns or Accredit Infrastructure Component

The accreditor reviews the infrastructure ISA documentation package and escalates security concerns or prepares and signs an accreditation letter. The accreditor submits the final package with recommendations to the executive sponsor.

4-4.4.6 Accept Residual Risk and Deploy Infrastructure Component

The executive sponsor accepts any residual risk by preparing and signing an acceptance letter, deploys the infrastructure component into production, and files the infrastructure ISA documentation package.

Exhibit 4-4
Phase 4, Evaluation


INPUT
ACTIVITIES
OUTPUT
Phase 3 Testing
IIA, Security Plan, Risk Assessment, Security Test and Evaluation Report
Evaluate ISA Documents and Prepare ISA Evaluation Report and Certification Letter
ISA Evaluation Report
Review ISA Documents, Prepare and Sign Certification Letter
Certification Letter
Signed Certification Letter
NO
Return to Applicable ISA Phase
YES
Business Requirements, Postal Service Issues, and ISA Documents
Analyze Documentation and Prepare Risk Mitigation Plan; and Prepare and Sign Accreditation Letter
Risk Mitigation Plan
Accreditation Letter
Accept Residual Risk
NO
Return to Applicable ISA Phase
YES
Deploy Infrastructure Component
File ISA Documentation
Phase 5 Production

4-5 Phase 5 – Production

Phase 5 encompasses activities that occur after the infrastructure component is deployed to the production environment and continue throughout the life cycle. (See Exhibit 4-5, Phase 5.)

4-5.1 Objectives

The objectives of this phase are to ensure protection of the infrastructure component after deployment and throughout its life cycle.

4-5.2 Deliverable

The deliverable for this phase is revised infrastructure ISA documentation.

4-5.3 Roles and Responsibilities

Roles	Responsibilities
Executive sponsor	Ensures secure operations and maintenance of the infrastructure component, including latest security patches and releases. Determines whether changes are significant and ensures that the infrastructure ISA process is reinitiated as required. Retires infrastructure component when no longer needed.
Program manager	Reviews existing security controls to determine whether they are still sufficient and implements additional or modifies existing security controls as required. Ensures that the infrastructure ISA documentation package is kept current.
ISSO	Provides guidance and consulting support.

4-5.4 Activities

4-5.4.1 Conduct Operations and Maintenance

Operate the infrastructure component with the security controls, processes, and procedures in place as documented in the infrastructure security plan, ensuring that they remain fully functional and unaltered by maintenance procedures. Ensure that the latest security software patches and releases are installed. The infrastructure component must be under configuration control and all changes properly documented.

4-5.4.2 Re-initiate Infrastructure ISA as Required

Re-initiate the infrastructure ISA every 3 years or if there is a significant change to the infrastructure component. Significant changes include a change to the level of *criticality* or *sensitivity* of hosted applications, a significant audit finding, or a significant security incident. Unresolved issues, new business requirements, new threats and vulnerabilities, operating environment changes, audit reports, and incidents must be appropriately addressed throughout the infrastructure component life cycle. Also, certain changes to the infrastructure component or its environment as well as business considerations could affect the security of the infrastructure and may require a re-initiation of the infrastructure ISA process. (See Chapter 5, Re-Initiating the Infrastructure ISA.)

4-5.4.3 Reassess Risks

Reassess risk every 3 years and whenever major changes are made to the infrastructure component, a serious breach occurs, or audit findings regarding security are issued.

4-5.4.4 Implement or Modify Security Controls

Monitor and test the security controls periodically and determine whether additional security controls need to be added or existing controls modified to properly secure the infrastructure component in the changing environment. If the infrastructure component security posture or controls change significantly, it is necessary to re-initiate the infrastructure ISA process.

4-5.4.5 Update Infrastructure ISA Documentation Package

Keep the infrastructure ISA documentation package current throughout the infrastructure component life cycle process.

4-5.4.6 Dispose of Equipment and Media

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

4-5.4.7 Retire Infrastructure Component

The infrastructure component may eventually be retired. Upon determination that an infrastructure component 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 infrastructure component in accordance with Handbook AS-805, *Information Security.*

Exhibit 4-5
Phase 5, Production

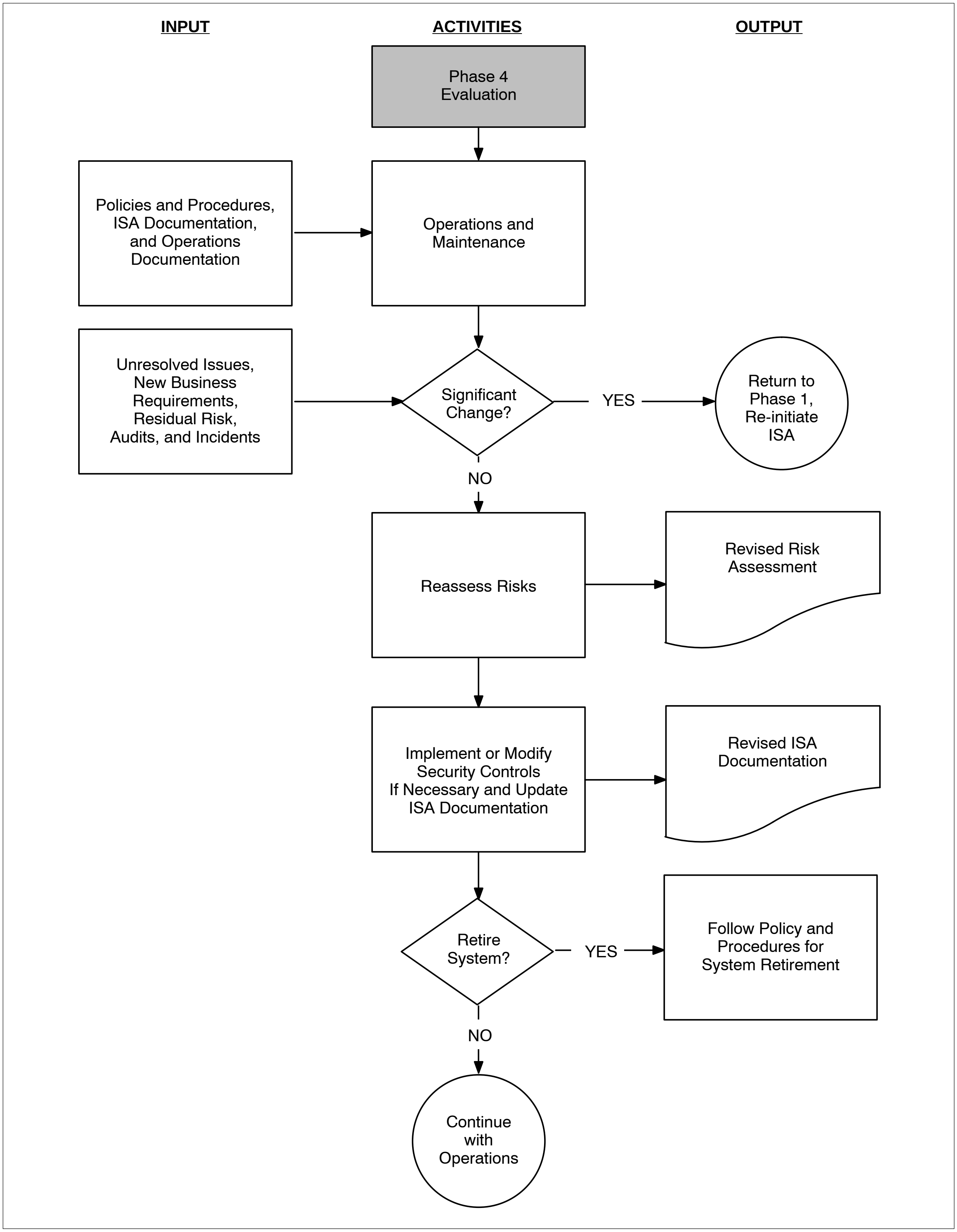

INPUT
ACTIVITIES
OUTPUT
Phase 4 Evaluation
Policies and Procedures, ISA Documentation, and Operations Documentation
Operations and Maintenance
Unresolved Issues, New Business Requirements, Residual Risk, Audits, and Incidents
Significant Change?
YES
Return to Phase 1, Re-initiate ISA
NO
Reassess Risks
Revised Risk Assessment
Implement or Modify Security Controls If Necessary and Update ISA Documentation
Revised ISA Documentation
Retire System?
YES
Follow Policy and Procedures for System Retirement
NO
Continue with Operations

Exhibit 4a

Infrastructure ISA Templates

Template Name	Applicability	Purpose
Infrastructure ISA Status Tracking Sheet	Optional use.	To record responsibility and schedule for completion for each infrastructure ISA product.
Infrastructure Impact Assessment	For infrastructure components.	To document sensitivity and criticality and to determine information security requirements for an infrastructure component.
Infrastructure Security Plan	For infrastructure components.	To create a blueprint for designing, building, and maintaining an infrastructure component that can be defended against threats and intruders, both internal and external.
Infrastructure Risk Assessment	For infrastructure components.	To identify assets at risk and their value and weaknesses and vulnerabilities, evaluate threats and vulnerabilities to determine risks, identify safeguards, analyze costs and benefits of safeguards, and document the residual risk.
Independent Risk Assessment Report	May be recommended if infrastructure component is publicly accessible; developed, hosted, managed primarily by non-Postal Service personnel; highly visible or has high impact. May be required at any time by VP/CTO or Mgr., CISO.	To provide a standard report format to document results of independent risk assessment, i.e., one conducted by an entity outside the development organization.
Infrastructure Security Test and Evaluation Plan	For infrastructure components.	To provide a framework for testing and evaluating the technical/nontechnical security controls/safeguards.
Infrastructure Security Test and Evaluation Report	For infrastructure components.	To document the results of the testing and evaluation of technical/nontechnical security controls/safeguards.
Infrastructure ISA Evaluation Report	For infrastructure components.	To document the ISSO evaluation of technical and nontechnical security features and other safeguards to establish extent to which an infrastructure component meets security requirements.
Certification Letter	For infrastructure components.	For the certifier to recommend approval for an infrastructure component to operate in given operational concept and environment at a documented level of residual risk.
Risk Mitigation Plan	For infrastructure components where residual risk is “High” or “Medium.”	To describe plan to mitigate residual risk, when such risk is “High” or “Medium” for infrastructure components and to provide a vehicle for the executive sponsor to accept the residual risk.
Accreditation Letter	For infrastructure components.	For the accreditor to recommend one of the following: accepting the infrastructure component 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.
Acceptance Letter	For infrastructure components.	For executive sponsor to accept residual risk.

5 Re-initiating The Infrastructure ISA

5-1 Purpose

The purpose of re-initiating the infrastructure ISA (Re-ISA) is to ensure that the following conditions are met:

a. Existing security controls and processes for the infrastructure component are still in place and functioning correctly.

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

c. Security controls and processes 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.

5-2 When Re-ISA Is Required

Re-ISA is required a minimum of every 3 years following the initial infrastructure ISA of the infrastructure component or for the following reasons:

a. Significant change to the operating environment, business requirements, or the infrastructure component. Any change that adversely affects the security of the infrastructure component is a significant change. Significant changes include but are not limited to:

   (1) Higher criticality or sensitivity designation of a hosted application.

   (2) Change from one major operation system to another.

   (3) Change in the hosting location, such as from a Postal Service facility to an outsourced, non-Postal Service location.

   (4) Change in the operating environment resulting from the discovery of a new vulnerability or threat that significantly alters the risk to the infrastructure component.

b. A significant information security incident that violates an explicit or implied security policy and compromises the integrity, availability, or confidentiality of a hosted application (e.g., a critical disruption or monetary loss, the unauthorized modification of sensitive or critical information, or the release of sensitive or business-controlled sensitivity information).

c. Significant finding of an audit or other external assessment.

d. A request by the VP/CTO; the manager, CISO; or the executive sponsor.

5-3 Process

5-3.1 Requesting a Re-ISA

Three years after an infrastructure component's ISA or for one of the other reasons previously covered, the manager, Information Security Assurance, requests a Re-ISA.

5-3.2 Conducting a Re-ISA

The deliverables from Phases 1 and 2 of the initial infrastructure ISA process should be reviewed, updated as required, signed, and dated. The Re-ISA follows the initial infrastructure ISA process with the following exceptions.

5-3.2.1 Phase 1, Definition

The following procedures are carried out under Phase 1 for the Re-ISA:

a. The high-level architecture diagram is updated as required.

b. The applications documented in the IIA are reviewed and updated in the IIA as required.

c. The security and privacy requirements are updated as required for the infrastructure component.

5-3.2.2 Phase 2, Design and Integration

The following procedures are carried out under Phase 2 for the Re-ISA:

a. New or modified security and privacy controls and processes are identified to satisfy any new or modified security requirements.

b. The new or modified security and privacy controls and processes are implemented.

c. The existing infrastructure security plan, infrastructure risk assessment, and standard operating procedures are updated to reflect these changes.

5-3.2.3 Phase 3, Testing

The following procedures are carried out under Phase 3 for the Re-ISA:

a. The infrastructure ST&E plan is updated as required.

b. Security testing is conducted based on the updated ST&E plan to ensure that the new or modified security and privacy controls and processes are functional and provide the appropriate level of protection for the infrastructure component.

c. The results of the security testing are documented in a ST&E report.

d. The operational security training materials are updated as required.

5-3.2.4 Phase 4, Evaluation

Phase 4 activities, focusing on the changes, are conducted as defined in Section 4-4.4.

5-3.2.5 Phase 5, Production

Phase 5 activities are conducted as defined in Section 4-5.4.

This page intentionally left blank