COURSE TECHNOLOGY
CENGAGE Learning™

Principles of Information Security, Fifth Edition

Chapter 10
Implementing Information Security

Change is good. You go first!

DILBERT (BY SCOTT ADAMS)

Learning Objectives

- Upon completion of this material, you should be able to:
  - Explain how an organization’s information security blueprint becomes a project plan
  - Discuss the many organizational considerations that a project plan must address
  - Explain the significance of the project manager’s role in the success of an information security project
  - Describe the need for professional project management for complex projects

Learning Objectives (cont'd)

- Describe technical strategies and models for implementing a project plan
- List and discuss the nontechnical problems that organizations face in times of rapid change

Introduction

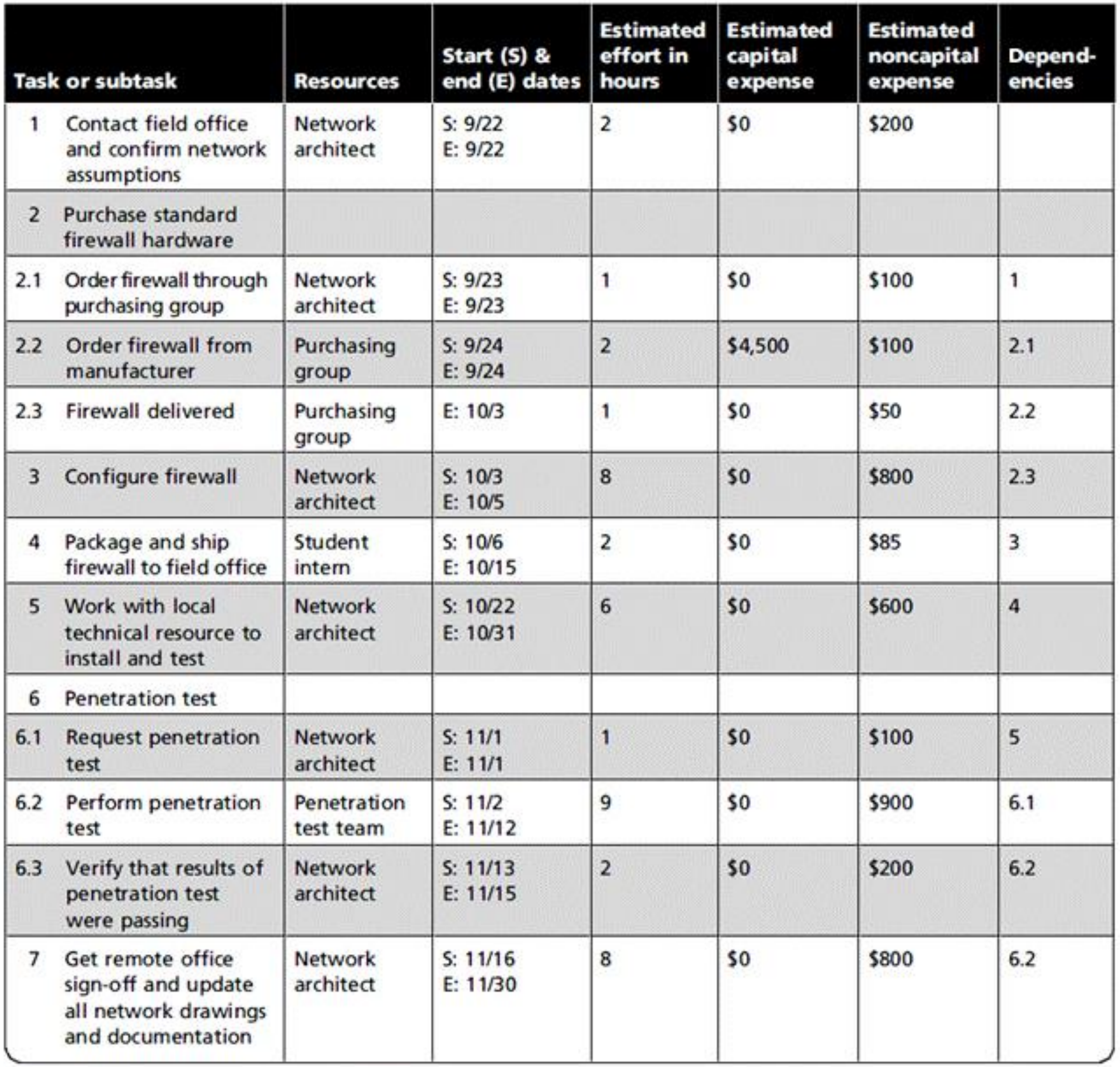
- SecSDLC implementation phase is accomplished by changing the configuration and operation of an organization’s information systems.
- Implementation includes changes to:
  - Procedures (through policy)
  - People (through training)
  - Hardware (through firewalls)
  - Software (through encryption)
  - Data (through classification)
- Organization translates blueprint for information security into a project plan.

Information Security Project Management

- Project plan must address project leadership, managerial/technical/budgetary considerations, and organizational resistance to change.
- Major steps in executing a project plan are:
  - Planning the project
  - Supervising tasks and action steps
  - Wrapping up
- Each organization must determine its own project management methodology for IT and information security projects.

Developing the Project Plan

- Creation of a project plan can be done using work breakdown structure (WBS).
- Major project tasks in WBS are:
  - Work to be accomplished
  - Assignees
  - Start and end dates
  - Amount of effort required
  - Estimated capital and noncapital expenses
  - Identification of dependencies between/among tasks
- Each major WBS task is further divided into smaller tasks or specific action steps.



Task or subtask	Resources	Start (S) & end (E) dates	Estimated effort in hours	Estimated capital expense	Estimated noncapital expense	Depend-encies
1 Contact field office and confirm network assumptions	Network architect	S: 9/22 E: 9/22	2	$0	$200	
2 Purchase standard firewall hardware						
2.1 Order firewall through purchasing group	Network architect	S: 9/23 E: 9/23	1	$0	$100	1
2.2 Order firewall from manufacturer	Purchasing group	S: 9/24 E: 9/24	2	$4,500	$100	2.1
2.3 Firewall delivered	Purchasing group	E: 10/3	1	$0	$50	2.2
3 Configure firewall	Network architect	S: 10/3 E: 10/5	8	$0	$800	2.3
4 Package and ship firewall to field office	Student intern	S: 10/6 E: 10/15	2	$0	$85	3
5 Work with local technical resource to install and test	Network architect	S: 10/22 E: 10/31	6	$0	$600	4
6 Penetration test						
6.1 Request penetration test	Network architect	S: 11/1 E: 11/1	1	$0	$100	5
6.2 Perform penetration test	Penetration test team	S: 11/2 E: 11/12	9	$0	$900	6.1
6.3 Verify that results of penetration test were passing	Network architect	S: 11/13 E: 11/15	2	$0	$200	6.2
7 Get remote office sign-off and update all network drawings and documentation	Network architect	S: 11/16 E: 11/30	8	$0	$800	6.2

Table 10-1 Example Project Plan Work Breakdown Structure

Project Planning Considerations

- As project plan is developed, adding detail is not always straightforward.
- Special considerations include financial, priority, time and schedule, staff, procurement, organizational feasibility, training and indoctrination, and scope.

Project Planning Considerations (cont’d)

- Financial considerations
  - Regardless of existing information security needs, the amount of effort that can be expended depends on available funds.
  - Cost-benefit analysis must be reviewed and verified prior to the development of a project plan.
  - Both public and private organizations have budgetary constraints, though of a different nature.
  - To justify an amount budgeted for a security project at either public or for-profit organizations, it may be useful to benchmark expenses of similar organizations.

Project Planning Considerations (cont’d)

- Priority considerations
  - In general, the most important information security controls should be scheduled first.
  - Implementation of controls is guided by prioritization of threats and value of threatened information assets.

Project Planning Considerations (cont'd)

- Time and scheduling considerations
  - Time impacts project plans at dozens of points, including:
    - Time to order, receive, install, and configure security control
    - Time to train the users
    - Time to realize control's return on investment

Project Planning Considerations (cont'd)

- Staffing considerations
  - Need for qualified, trained, and available personnel constrains project plan
  - Experienced staff is often needed to implement technologies and develop and implement policies and training programs.
- Procurement considerations
  - Often constraints on the selection of equipment/services
    - Some organizations require use of particular service vendors/manufacturers/suppliers.
  - These constraints may limit which technologies can be acquired.

Project Planning Considerations (cont'd)

- Organizational feasibility considerations
  - Changes should be transparent to system users unless the new technology is intended to change procedures (e.g., requiring additional authentication or verification).
  - Successful project requires that organization be able to assimilate proposed changes.
  - New technologies sometimes require new policies, employee training, and education.

Project Planning Considerations (cont’d)

- Training and indoctrination considerations
  - Size of organization and normal conduct of business may preclude a large training program for new security procedures/technologies.
  - If so, the organization should conduct phased-in or pilot implementation.

Project Planning Considerations (cont’d)

- Scope considerations
  - Project scope: description of project’s features, capabilities, functions, and quality level, used as the basis of a project plan
  - Organizations should implement large information security projects in stages.

The Need for Project Management

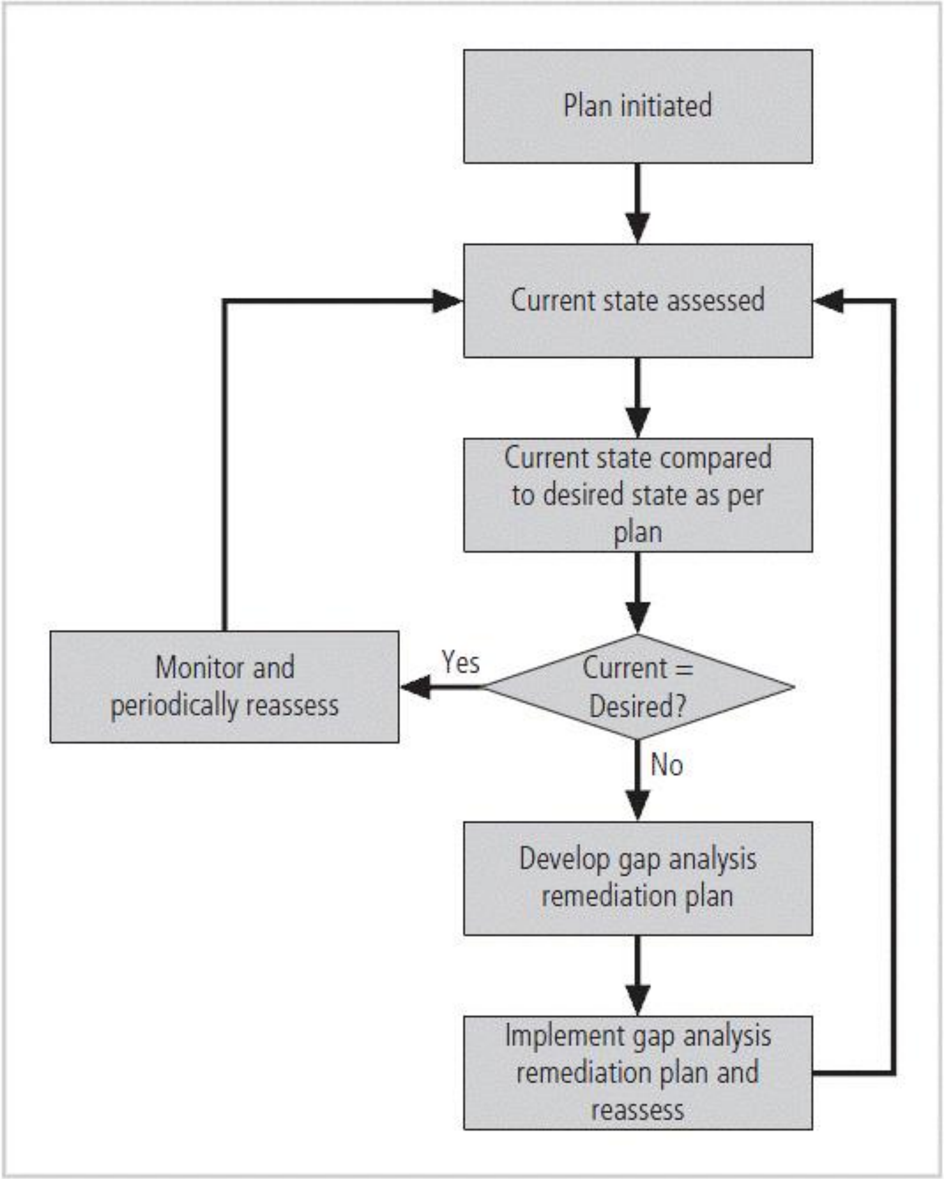
- Project management requires a unique set of skills and thorough understanding of a broad body of specialized knowledge.
- Most information security projects require a trained project manager (a CISO) or skilled IT manager trained in project management techniques.

The Need for Project Management (cont’d)

- Supervised implementation
  - Some organizations may designate a champion from general management community of interest to supervise implementation of information security project plan.
  - An alternative is to designate a senior IT manager or CIO to lead implementation.
  - Best solution is to designate a suitable person from information security community of interest.
  - In final analysis, each organization must find project leadership best suited to its specific needs.

The Need for Project Management (cont'd)

- Executing the plan
  - A negative feedback loop ensures that project progress is measured periodically.
    - When significant deviation occurs, corrective action is taken.
  - Often, a project manager can adjust one of three planning parameters for the task being corrected:
    - Effort and money allocated
    - Elapsed time/Scheduling impact
    - Quality or quantity of deliverable


Plan initiated
Current state assessed
Current state compared to desired state as per plan
Current = Desired?
Yes
No
Monitor and periodically reassess
Develop gap analysis remediation plan
Implement gap analysis remediation plan and reassess

© Cengage Learning 2015

Figure 10-1 Gap analysis

The Need for Project Management (cont'd)

- Project wrap-up
  - Project wrap-up is usually handled as procedural task and assigned to mid-level IT or information security manager.
  - Collect documentation, finalize status reports, and deliver final report and presentation at wrap-up meeting
  - Goal of wrap-up is to resolve any pending issues, critique overall project effort, and draw conclusions about how to improve process.

Security Project Management Certifications

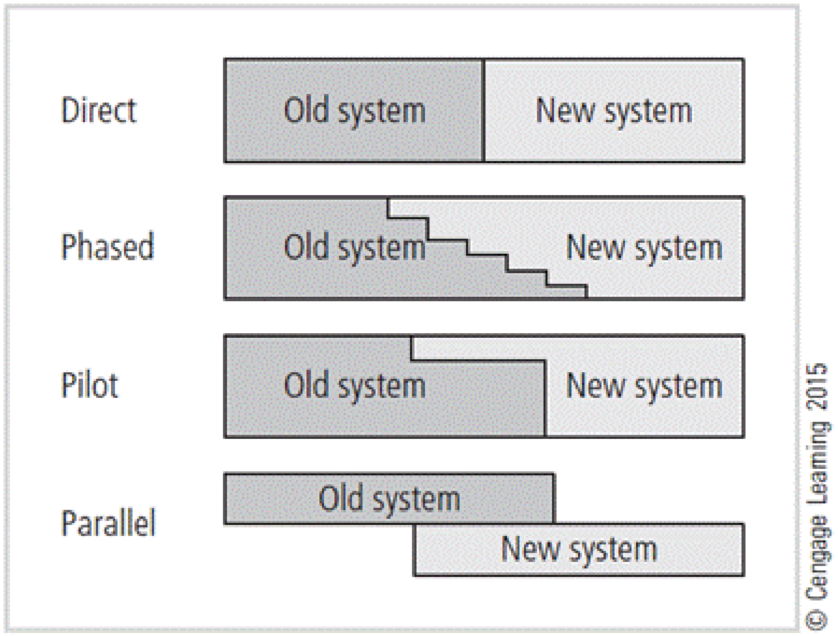
- GIAC certified project manager
  - Offered by SANS Institute; focuses on security professionals/managers with project management responsibilities
- IT security project management
  - Offered by EC Council as a milestone in its Certified E-Business Professional program
- Certified security project manager
  - Security Industry Association focused on physical security; also incorporates information security

Technical Aspects of Implementation

- Some aspects of implementation process are technical and deal with the application of technology.
  - Others deal with human interface to technical systems.

Conversion Strategies

- As components of new security system are planned, provisions must be made for changeover from the previous method of performing a task to the new method.
- Four basic approaches:
  - Direct changeover
  - Phased implementation
  - Pilot implementation
  - Parallel operations

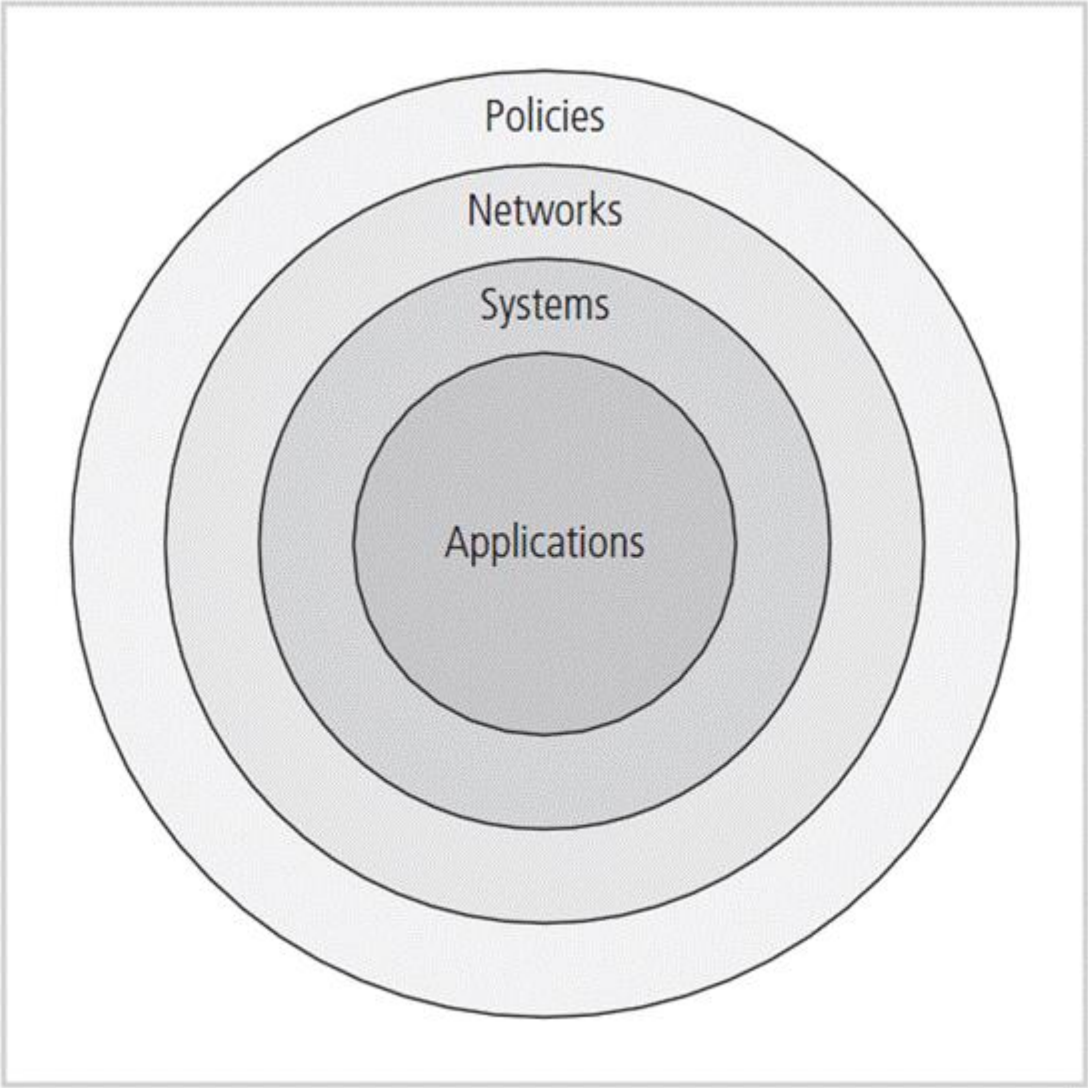


© Cengage Learning 2015

Figure 10-2 Conversion strategies

The Bull’s-Eye Model

- Proven method for prioritizing program of complex change
- Requires that issues be addressed from general to specific; focus is on systematic solutions and not on individual problems
- Relies on the process of project plan evaluation in four layers:
  - Policies
  - Networks
  - Systems
  - Applications



© Cengage Learning 2015

Figure 10-3 The bull's-eye model

To Outsource or Not

- Just as some organizations outsource IT operations, organizations can outsource part or all of their information security programs.
- When an organization outsources most/all IT services, information security should be part of contract arrangement with the supplier.
- Organizations of all sizes frequently outsource network monitoring functions.

Technology Governance and Change Control

- Technology governance guides how frequently technical systems are updated and how updates are approved/funded.
- By managing the process of change, the organization can:
  - Improve communication, enhance coordination, reduce unintended consequences, improve quality of service, and ensure groups are complying with policies

Nontechnical Aspects of Implementation

- Some aspects of implementation are not technical in nature, instead dealing with the human interface to technical systems.
- Include creating a culture of change management and considerations for the organizations facing change.

The Culture of Change Management

- Prospect of change can cause employees to consciously or unconsciously resist the change.
- The stress of change can increase the probability of mistakes or create vulnerabilities in systems.
- Change management can lower resistance to change and build resilience.
- Lewin change model:
  - Unfreezing
  - Moving
  - Refreezing

Considerations for Organizational Change

- Steps can be taken to make employees more amenable to change:
  - Reducing resistance to change from the start
  - Developing a culture that supports change

Considerations for Organizational Change (cont'd)

- Reducing resistance to change from the start
  - The more ingrained the existing methods and behaviors, the more difficult the change.
  - Best to improve interaction between affected members of organization and project planners in early project phases
  - Three-step process for project managers: communicate, educate, and involve
  - Joint application development

Considerations for Organizational Change (cont'd)

- Developing a culture that supports change
  - Ideal organization fosters resilience to change
  - Resilience: An organization understands change is a necessary part of the organizational culture, and embracing change is more productive than fighting it.
  - To develop such a culture, the organization must successfully accomplish many projects that require change.

Information Systems Security Certification and Accreditation

- It may seem that only systems handling secret government data require security certification and accreditation.
- In order to comply with recent federal regulations protecting personal privacy, the organizations need to have formal mechanisms for verification and validation.

Information Systems Security Certification and Accreditation (cont'd)

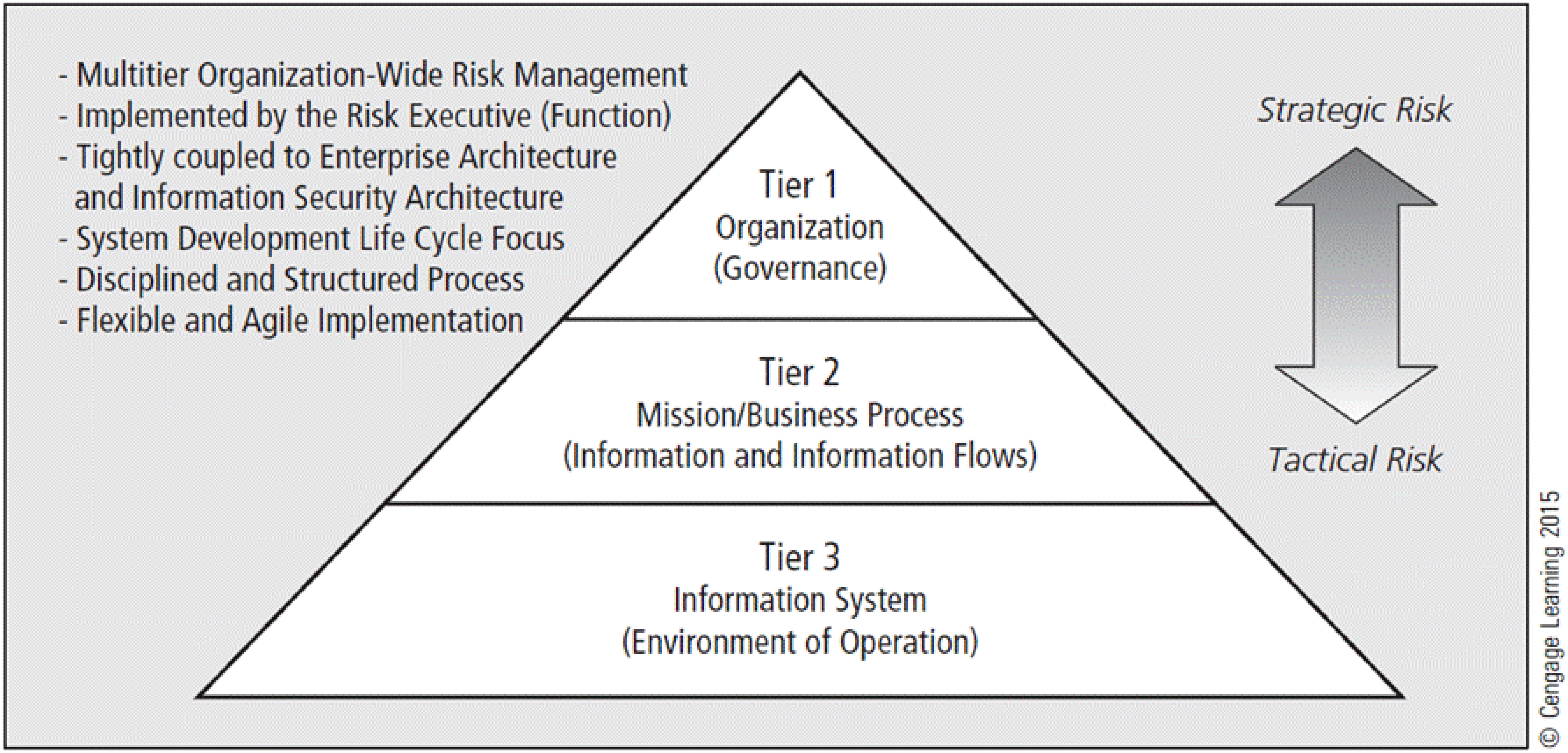
- Certification versus accreditation
  - Accreditation: authorizes IT system to process, store, or transmit information; assures systems of adequate quality
  - Certification: evaluation of technical and nontechnical security controls of IT system establishing extent to which design and implementation meet security requirements

The NIST Security Life Cycle Approach

- SP 800-37, Rev. 1: *Guidelines for Applying the Risk Management Framework to Federal Information Systems*, and CNSS Instruction-1000: *National Information Assurance Certification and Accreditation Process* (NIACAP)
  - Provide guidance for the certification and accreditation of federal information systems
- Information processed by the federal government is grouped into one of three categories:
  - National security information (NSI)
  - Non-NSI
  - Intelligence community (IC)

The NIST Security Life Cycle Approach (cont'd)

- A new publication, NIST SP 800-39: *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information Systems View* builds on a three-tiered approach to risk management
  - Tier 1 addresses risk from organizational perspective
  - Tier 2 addresses risk from mission/business process perspective
  - Tier 3 addresses risk from information system perspective



- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation

© Cengage Learning 2015

Figure 10-4 Tiered Risk Management Framework

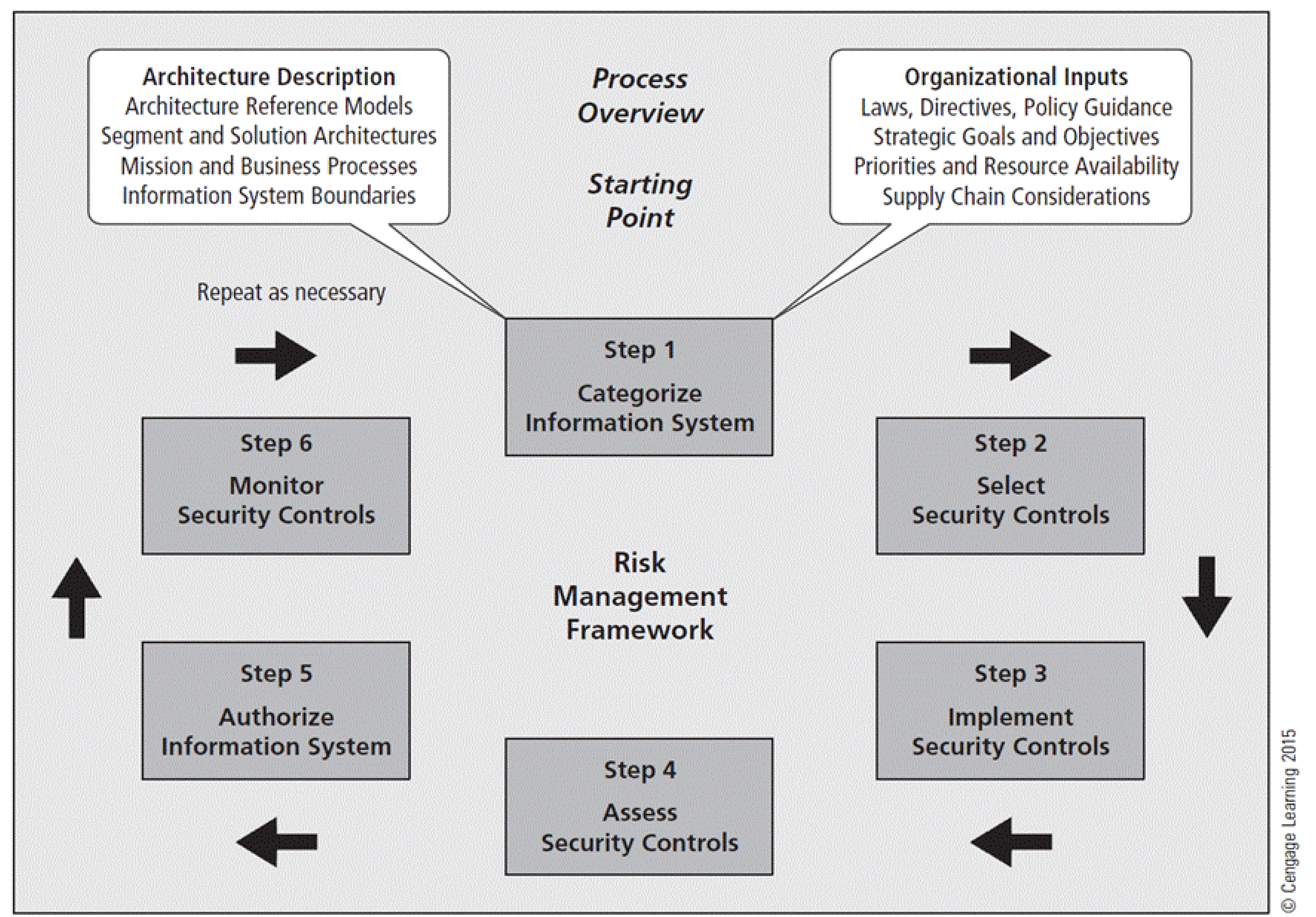

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
Process Overview
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1
Categorize Information System
Step 2
Select Security Controls
Step 3
Implement Security Controls
Step 4
Assess Security Controls
Step 5
Authorize Information System
Step 6
Monitor Security Controls
Risk Management Framework

Figure 10-5 Risk Management Framework

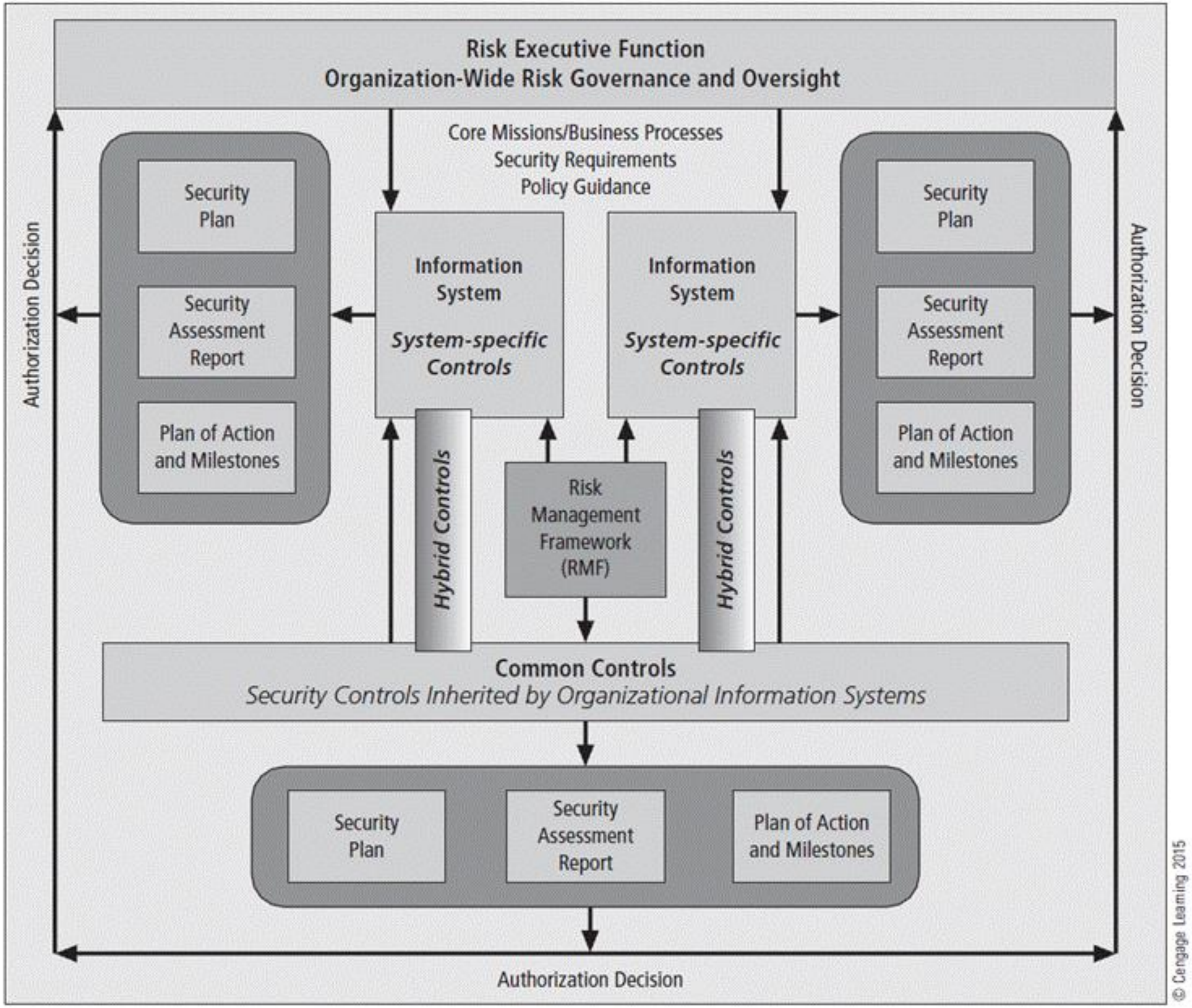

Risk Executive Function
Organization-Wide Risk Governance and Oversight
Core Missions/Business Processes
Security Requirements
Policy Guidance
Authorization Decision
Security Plan
Security Assessment Report
Plan of Action and Milestones
Information System
System-specific Controls
Information System
System-specific Controls
Security Plan
Security Assessment Report
Plan of Action and Milestones
Authorization Decision
Hybrid Controls
Risk Management Framework (RMF)
Hybrid Controls
Common Controls
Security Controls Inherited by Organizational Information Systems
Security Plan
Security Assessment Report
Plan of Action and Milestones
Authorization Decision
© Cengage Learning 2015

Figure 10-6 Security control allocation from NIST SP 800-37, Rev. 1

NSTISS Certification and Accreditation

- National security interest systems have their own C&A standards
- NSTISS Instruction 1000: National Information Assurance Certification and Accreditation Process (NIACAP)
  - Establishes minimum national standards for certifying/accrediting national security systems
  - Designed to certify that IS meets documented requirements
  - Composed of four phases: definition, verification, validation, and post accreditation

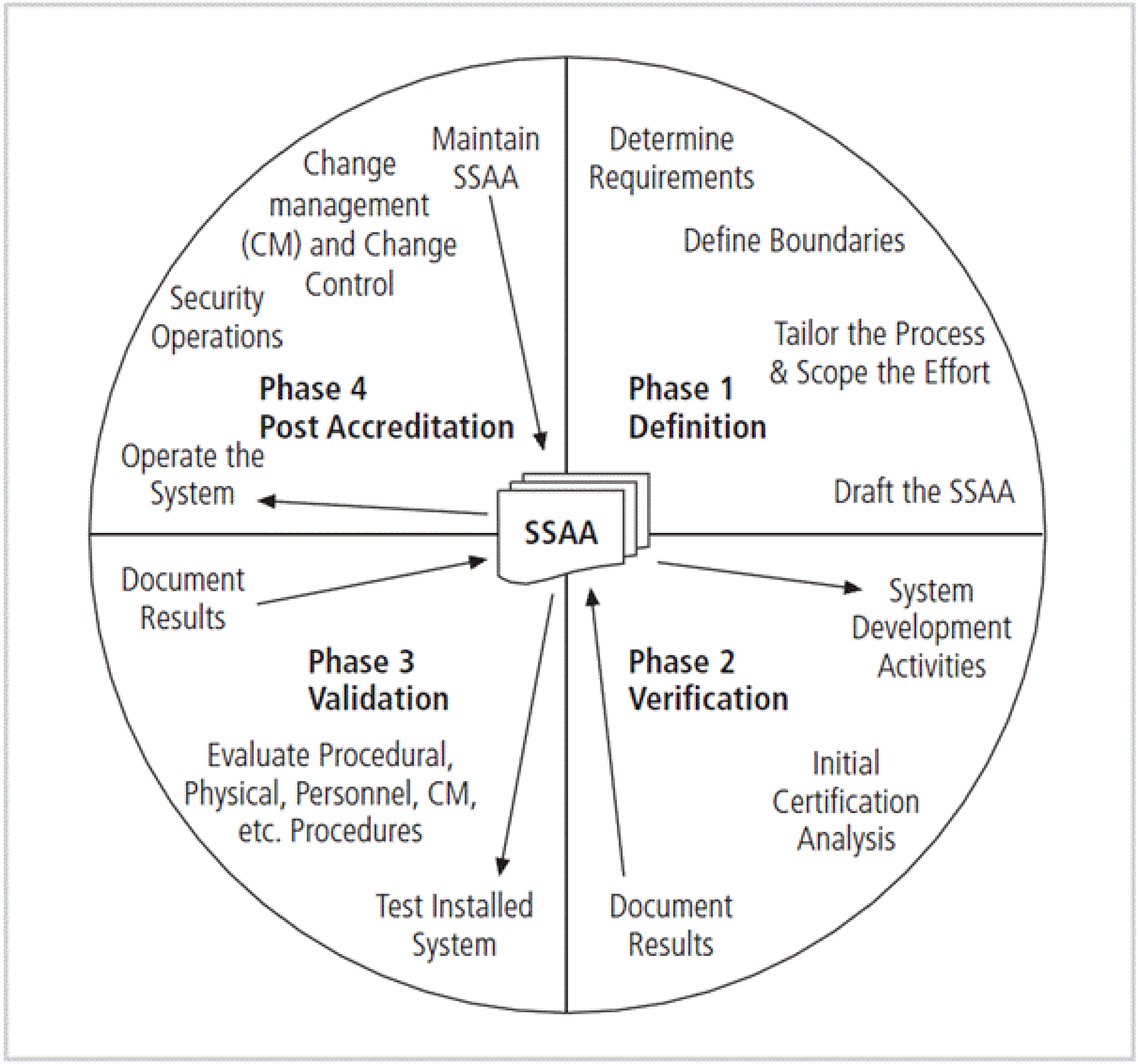
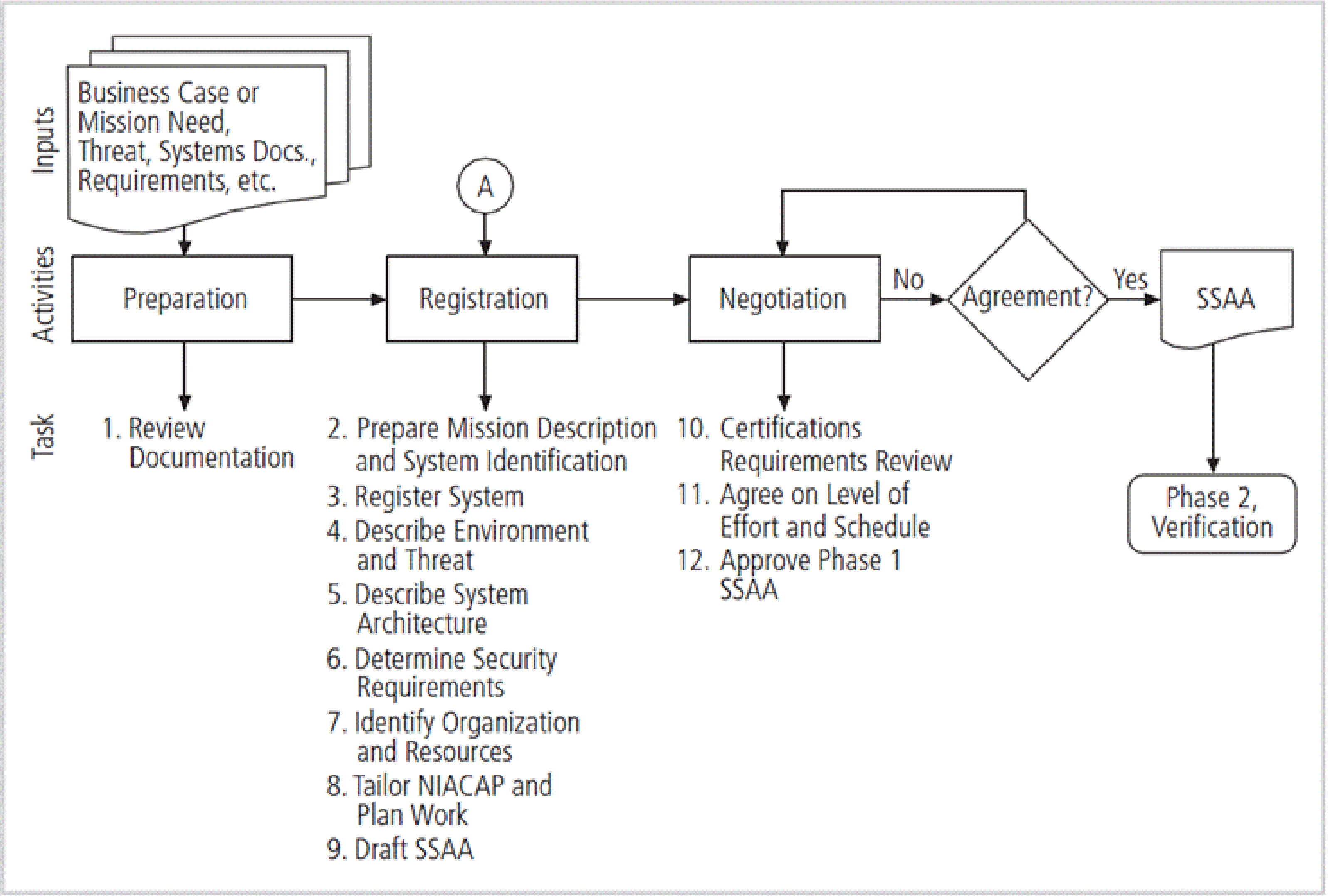

Maintain SSAA
Change management (CM) and Change Control
Security Operations
Phase 4 Post Accreditation
Operate the System
Determine Requirements
Define Boundaries
Tailor the Process & Scope the Effort
Phase 1 Definition
Draft the SSAA
SSAA
Document Results
Phase 3 Validation
Evaluate Procedural, Physical, Personnel, CM, etc. Procedures
Test Installed System
System Development Activities
Phase 2 Verification
Initial Certification Analysis
Document Results

Figure 10-7 Overview of the NIACAP process

Source: NSTISSI-1000.



Inputs

Business Case or Mission Need, Threat, Systems Docs., Requirements, etc.

Activities

A

Preparation

Registration

Negotiation

No

Agreement?

Yes

SSAA

Task

1. Review Documentation

2. Prepare Mission Description and System Identification
3. Register System
4. Describe Environment and Threat
5. Describe System Architecture
6. Determine Security Requirements
7. Identify Organization and Resources
8. Tailor NIACAP and Plan Work
9. Draft SSAA

10. Certifications Requirements Review
11. Agree on Level of Effort and Schedule
12. Approve Phase 1 SSAA

Phase 2, Verification

Figure 10-8 NIACAP Phase 1, Definition

Source: NSTISSI-1000.

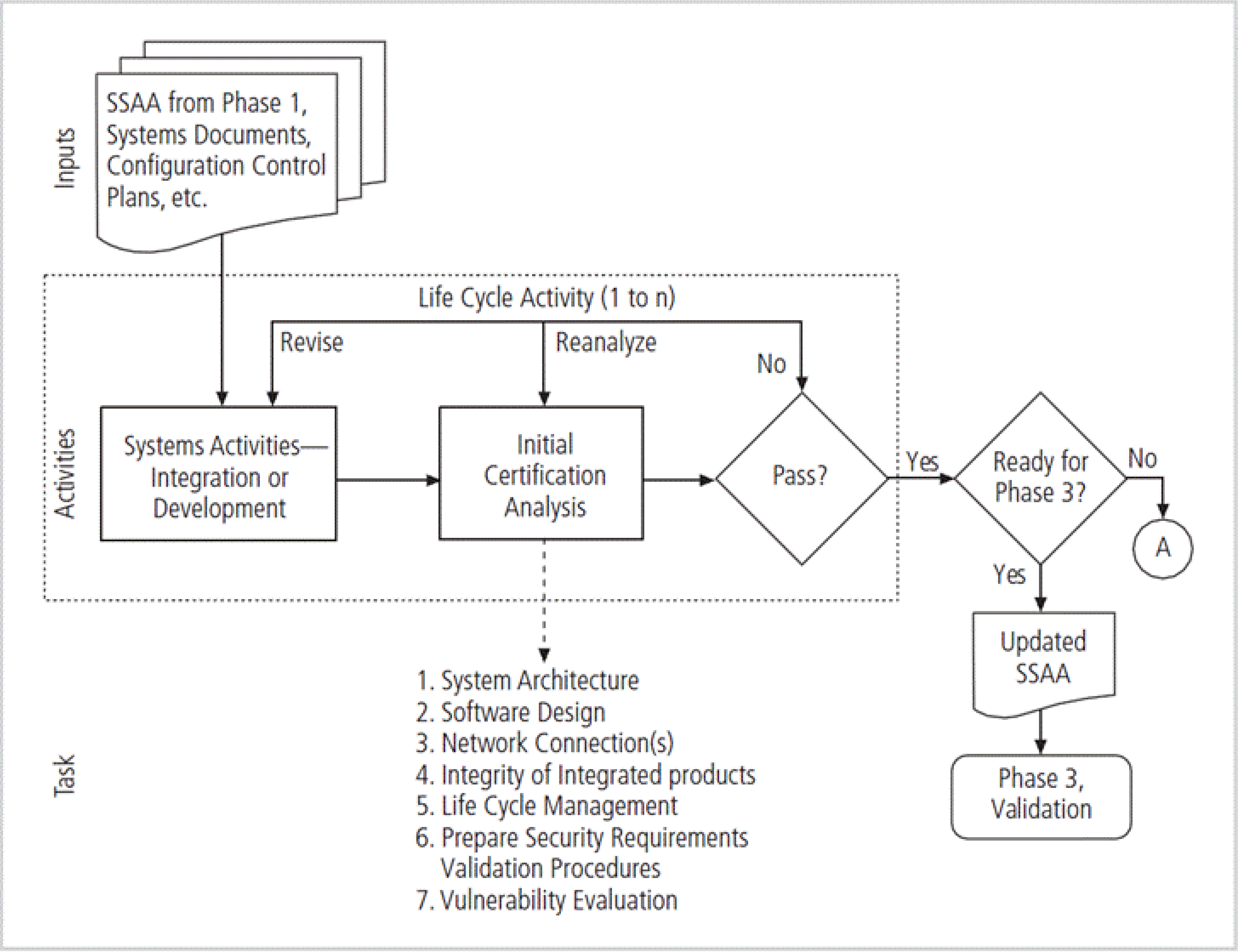
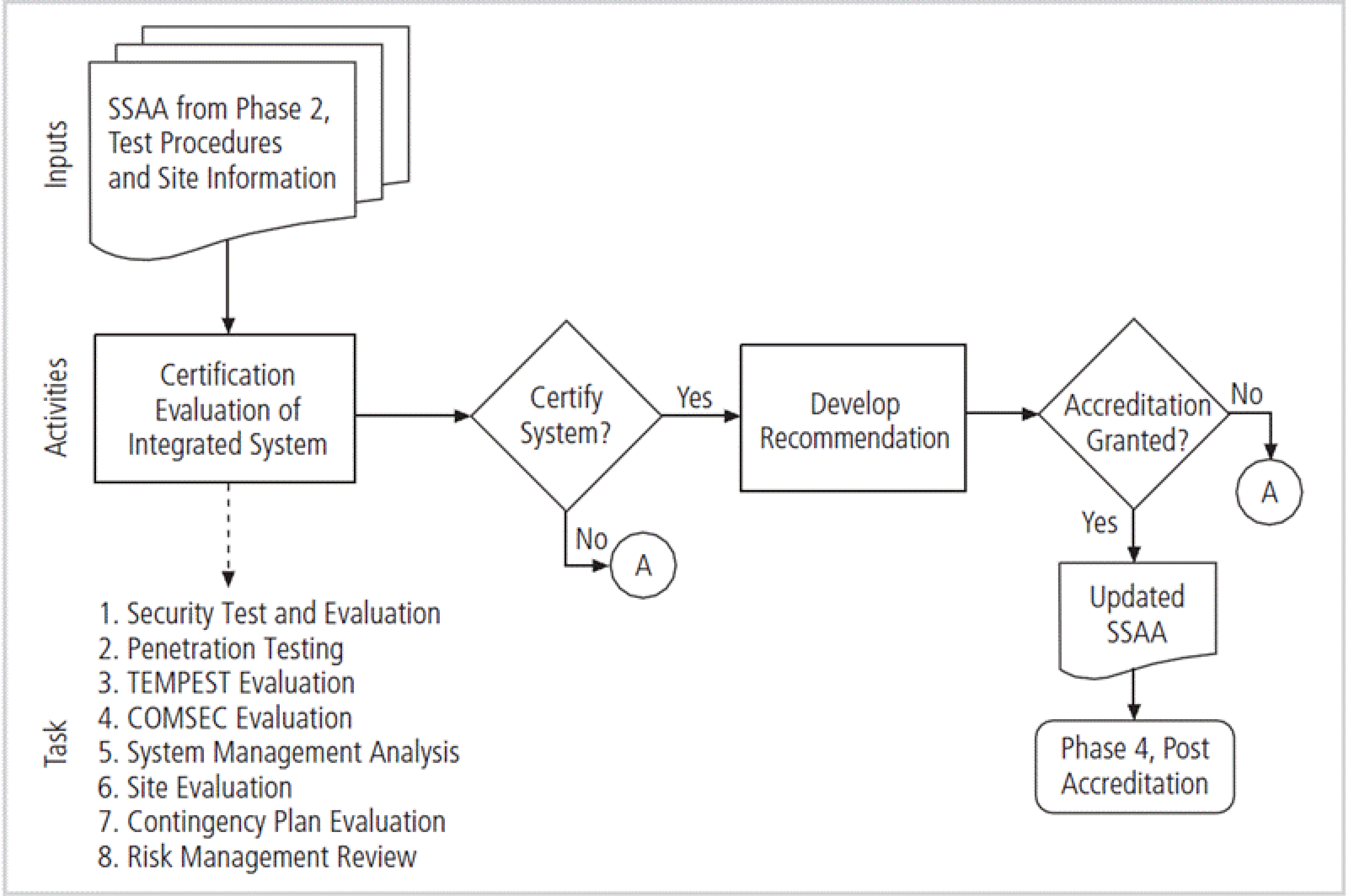

Inputs
SSAA from Phase 1, Systems Documents, Configuration Control Plans, etc.
Life Cycle Activity (1 to n)
Revise
Reanalyze
No
Activities
Systems Activities—Integration or Development
Initial Certification Analysis
Pass?
Yes
Ready for Phase 3?
No
A
Yes
Updated SSAA
Phase 3, Validation
Task
1. System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

Figure 10-9 NIACAP Phase 2, Verification

Source: NSTISSI-1000.



Inputs

SSAA from Phase 2, Test Procedures and Site Information

Activities

Certification Evaluation of Integrated System

Certify System?

Yes

No

A

Develop Recommendation

Accreditation Granted?

No

A

Yes

Updated SSAA

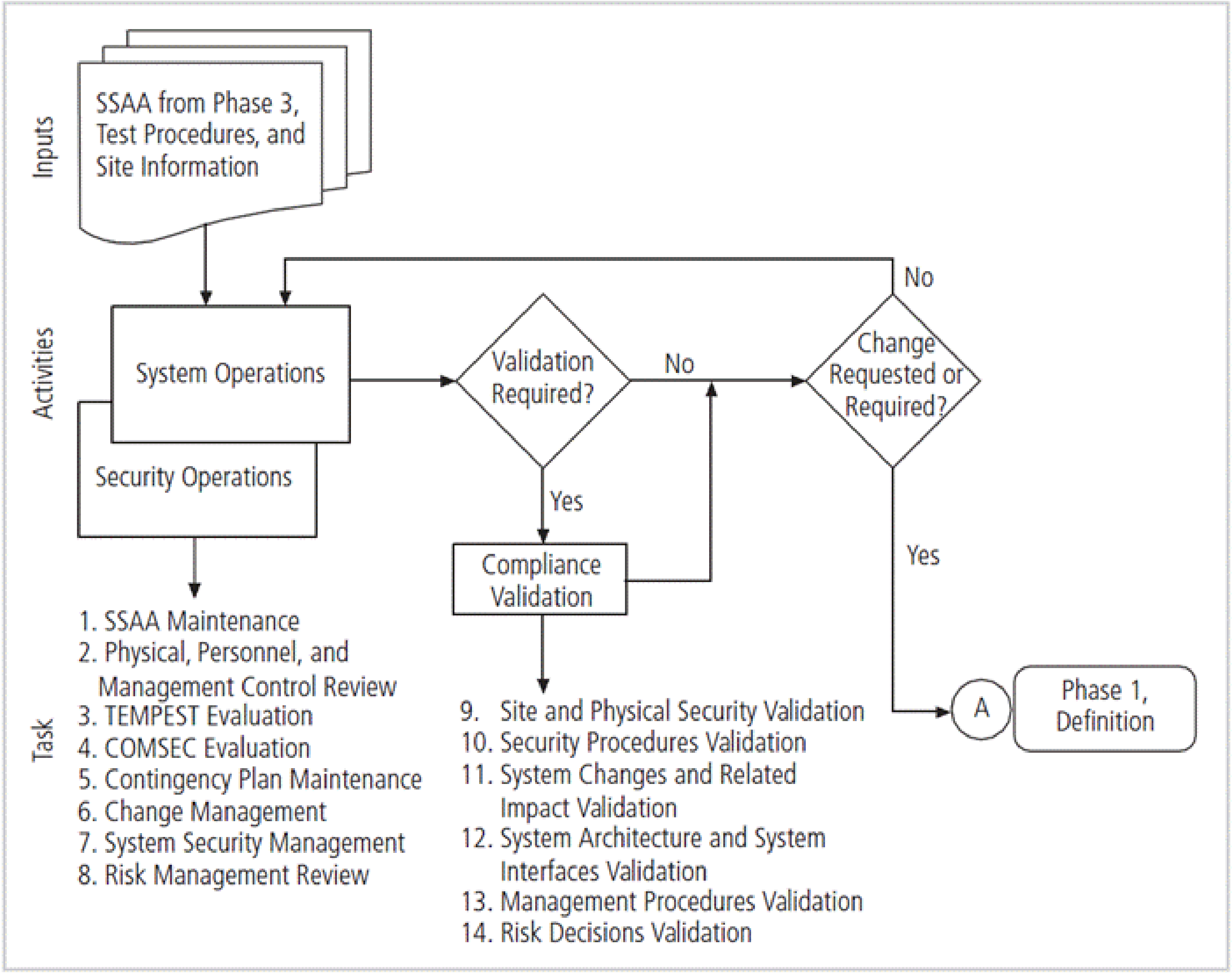
Phase 4, Post Accreditation

Task

1. Security Test and Evaluation
2. Penetration Testing
3. TEMPEST Evaluation
4. COMSEC Evaluation
5. System Management Analysis
6. Site Evaluation
7. Contingency Plan Evaluation
8. Risk Management Review

Figure 10-10 NIACAP Phase 3, Validation

Source: NSTISSI-1000.



Inputs

SSAA from Phase 3, Test Procedures, and Site Information

Activities

System Operations

Security Operations

Validation Required?

No

Yes

Compliance Validation

Change Requested or Required?

No

Yes

A

Phase 1, Definition

Task

1. SSAA Maintenance
2. Physical, Personnel, and Management Control Review
3. TEMPEST Evaluation
4. COMSEC Evaluation
5. Contingency Plan Maintenance
6. Change Management
7. System Security Management
8. Risk Management Review

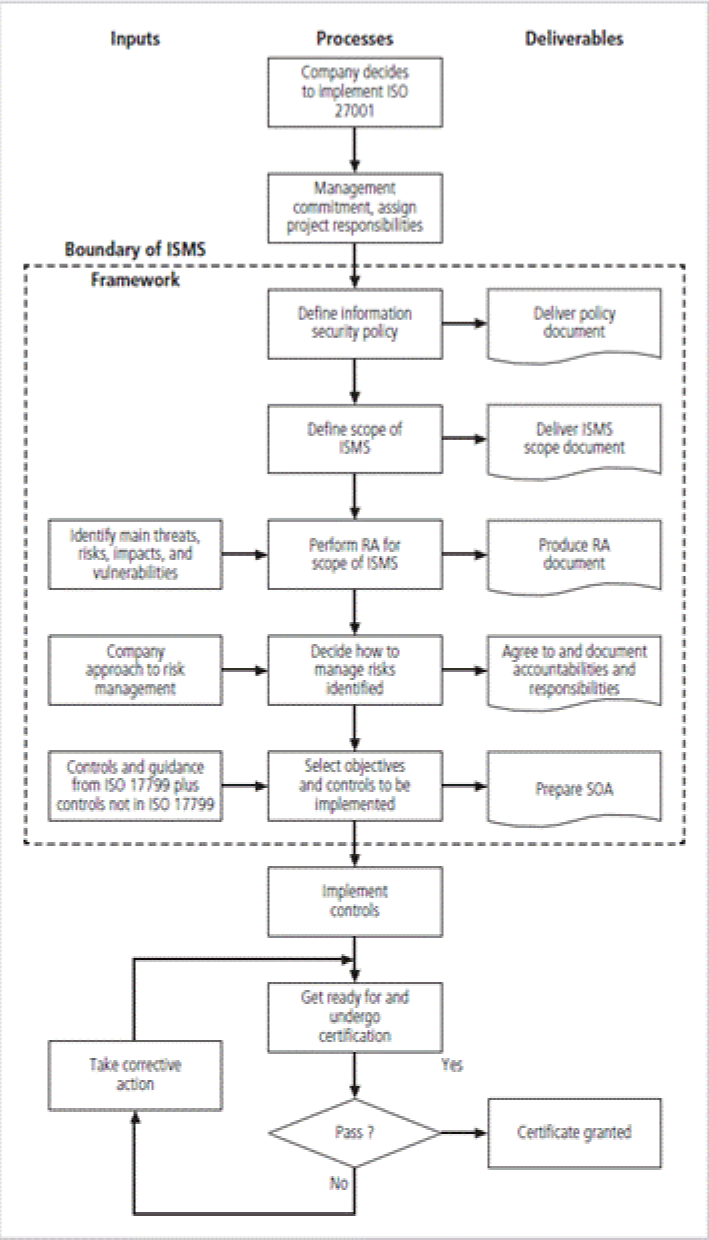
9. Site and Physical Security Validation
10. Security Procedures Validation
11. System Changes and Related Impact Validation
12. System Architecture and System Interfaces Validation
13. Management Procedures Validation
14. Risk Decisions Validation

Figure 10-11 NIACAP Phase 4, Post Accreditation

Source: NSTISSI-1000.

ISO 27001/ 27002 Systems Certification and Accreditation

- Organizations outside the United States apply these standards.
- Standards were originally created to provide a foundation for British certification of information security management systems (ISMSs).
- Organizations wishing to demonstrate their systems have met this international standard must follow the certification process.


Inputs
Processes
Deliverables
Company decides to implement ISO 27001
Management commitment, assign project responsibilities
Boundary of ISMS
Framework
Define information security policy
Deliver policy document
Define scope of ISMS
Deliver ISMS scope document
Identify main threats, risks, impacts, and vulnerabilities
Perform RA for scope of ISMS
Produce RA document
Company approach to risk management
Decide how to manage risks identified
Agree to and document accountabilities and responsibilities
Controls and guidance from ISO 17799 plus controls not in ISO 17799
Select objectives and controls to be implemented
Prepare SOA
Implement controls
Get ready for and undergo certification
Take corrective action
Yes
Pass ?
Certificate granted
No

© Cengage Learning 2015

Figure 10-12 ISMS certification and accreditation[11]

Summary

- Moving from security blueprint to project plan
- Organizational considerations addressed by project plan
- Project manager’s role in the success of an information security project
- Technical strategies and models for implementing project plan
- Nontechnical problems that organizations face in times of rapid change