COURSE TECHNOLOGY
CENGAGE Learning™

Principles of Information Security, Fourth 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
  - Enumerate 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
  - Establish the need for professional project management for complex projects

Learning Objectives (cont'd.)

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

Introduction

- SecSDLC implementation phase is accomplished through changing configuration and operation of 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 concrete project plan

Information Security Project Management

- Once organization's vision and objectives are understood, process for creating project plan can be defined
- Major steps in executing 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 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 and End Dates	Estimated Effort in Hours	Estimated Capital Expense	Estimated Noncapital Expense	Depen-dencies
1	Contact field office and confirm network assumptions	Network architect	S: 9/22 E:	2	0	200	
2	Purchase standard firewall hardware	Network architect and purchasing group	S: E:	4	4,500	250	1
3	Configure firewall	Network architect	S: E:	8	0	800	2
4	Package and ship to field office	Student intern	S: E: 10/15	2	0	85	3
5	Work with local technical resource to install and test firewall	Network architect	S: E:	6	0	600	4
6	Complete vulnerability assessment by penetration test team	Network architect and penetration test team	S: E:	12	0	1,200	5
7	Get remote office sign-off and update all network drawings and documentation	Network architect	S: E: 11/30	8	0	800	6

Table 10-1 Example Project Plan Work Breakdown Structure–Early Draft

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, and training

Project Planning Considerations (cont'd.)

- Financial considerations
  - No matter what information security needs exist, the amount of effort that can be expended depends on funds available
  - Cost benefit analysis must be verified prior to development of 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 dozens of points in the development of a project plan, including:
    - Time to order, receive, install, and configure security control
    - Time to train the users
    - Time to realize return on investment of control

Project Planning Considerations (cont'd.)

- Staffing considerations
  - Lack of enough qualified, trained, and available personnel constrains project plan
  - Experienced staff is often needed to implement available technologies and develop and implement policies and training programs

Project Planning Considerations (cont'd.)

- Procurement considerations
  - IT and information security planners must consider acquisition of goods and services
  - Many constraints on selection process for equipment and services in most organizations, specifically in selection of service vendors or products from manufacturers/suppliers
  - These constraints may eliminate a technology from realm of possibilities

Project Planning Considerations (cont'd.)

- Organizational feasibility considerations
  - Policies require time to develop; new technologies require time to be installed, configured, and tested
  - Employees need training on new policies and technology, and how new information security program affects their working lives
  - Changes should be transparent to system users unless the new technology is intended to change procedures (e.g., requiring additional authentication or verification)

Project Planning Considerations (cont'd.)

- Training and indoctrination considerations
  - Size of organization and normal conduct of business may preclude a single large training program on new security procedures/technologies
  - Thus, organization should conduct phased-in or pilot approach to implementation

Scope Considerations

- Project scope: concerns boundaries of time and effort-hours needed to deliver planned features and quality level of project deliverables
- In the case of information security, project plans should not attempt to implement the entire security system at one time

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 versed in project management techniques

The Need for Project Management (cont'd.)

- Supervised implementation
  - Some organizations may designate champion from general management community of interest to supervise implementation of information security project plan
  - An alternative is to designate senior IT manager or CIO to lead implementation
  - Optimal solution is to designate a suitable person from information security community of interest
  - It is up to each organization to find the most suitable leadership for a successful project implementation

The Need for Project Management (cont'd.)

- Executing the plan
  - Negative feedback ensures project progress is measured periodically
    - Measured results compared against expected results
    - When significant deviation occurs, corrective action taken
  - Often, project manager can adjust one of three parameters for task being corrected:
    - Effort and money allocated
    - Scheduling impact
    - Quality or quantity of deliverable

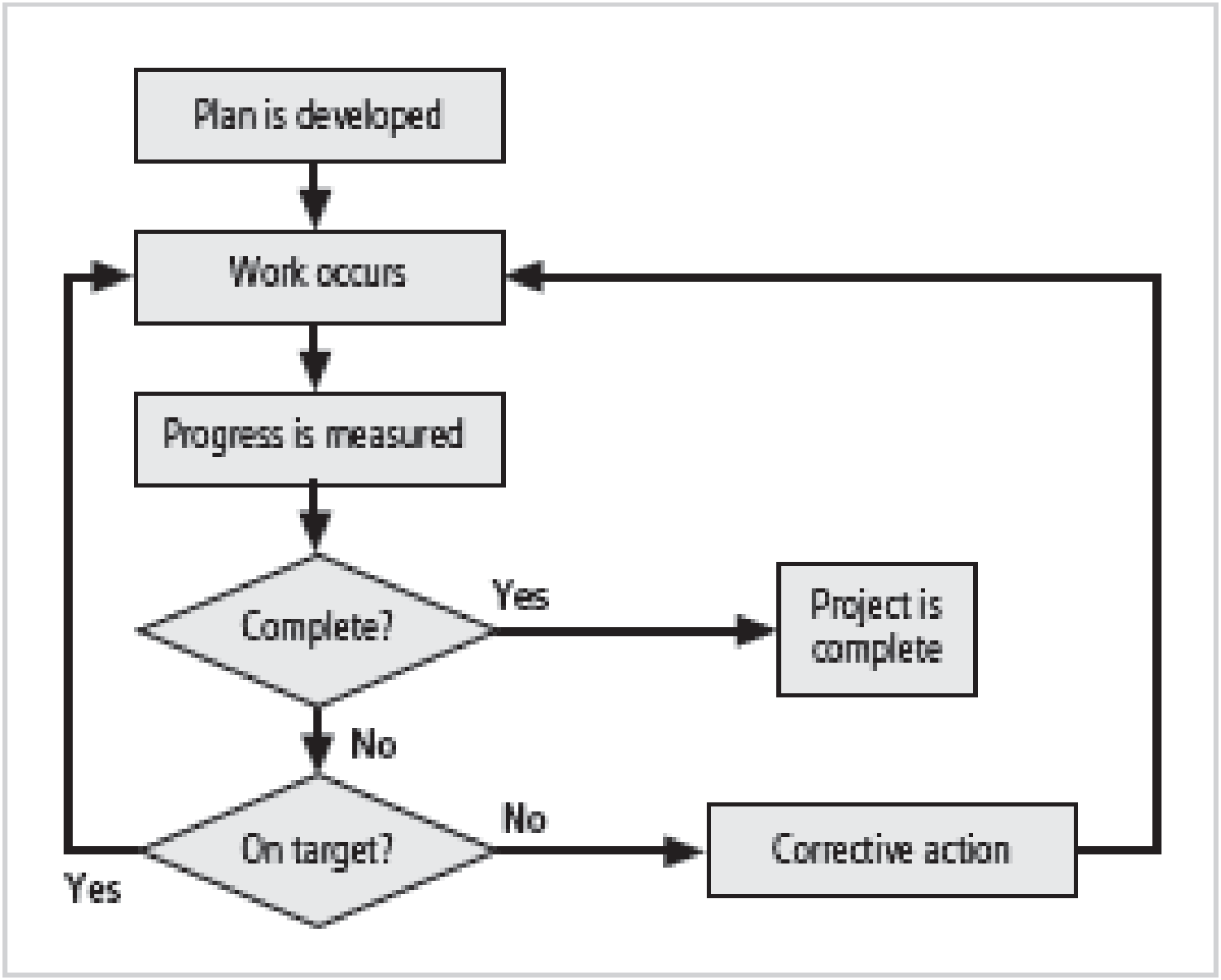

Figure 10-1 Negative Feedback Loop

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

Technical Aspects of Implementation

- Some parts of implementation process are technical in nature, dealing with application of technology
- Others are not, dealing instead with human interface to technical systems

Conversion Strategies

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

The Bull's-Eye Model

- Proven method for prioritizing program of complex change
- Issues addressed from general to specific; focus is on systematic solutions and not individual problems
- Relies on process of evaluating project plans in progression through four layers:
  - Policies
  - Networks
  - Systems
  - Applications

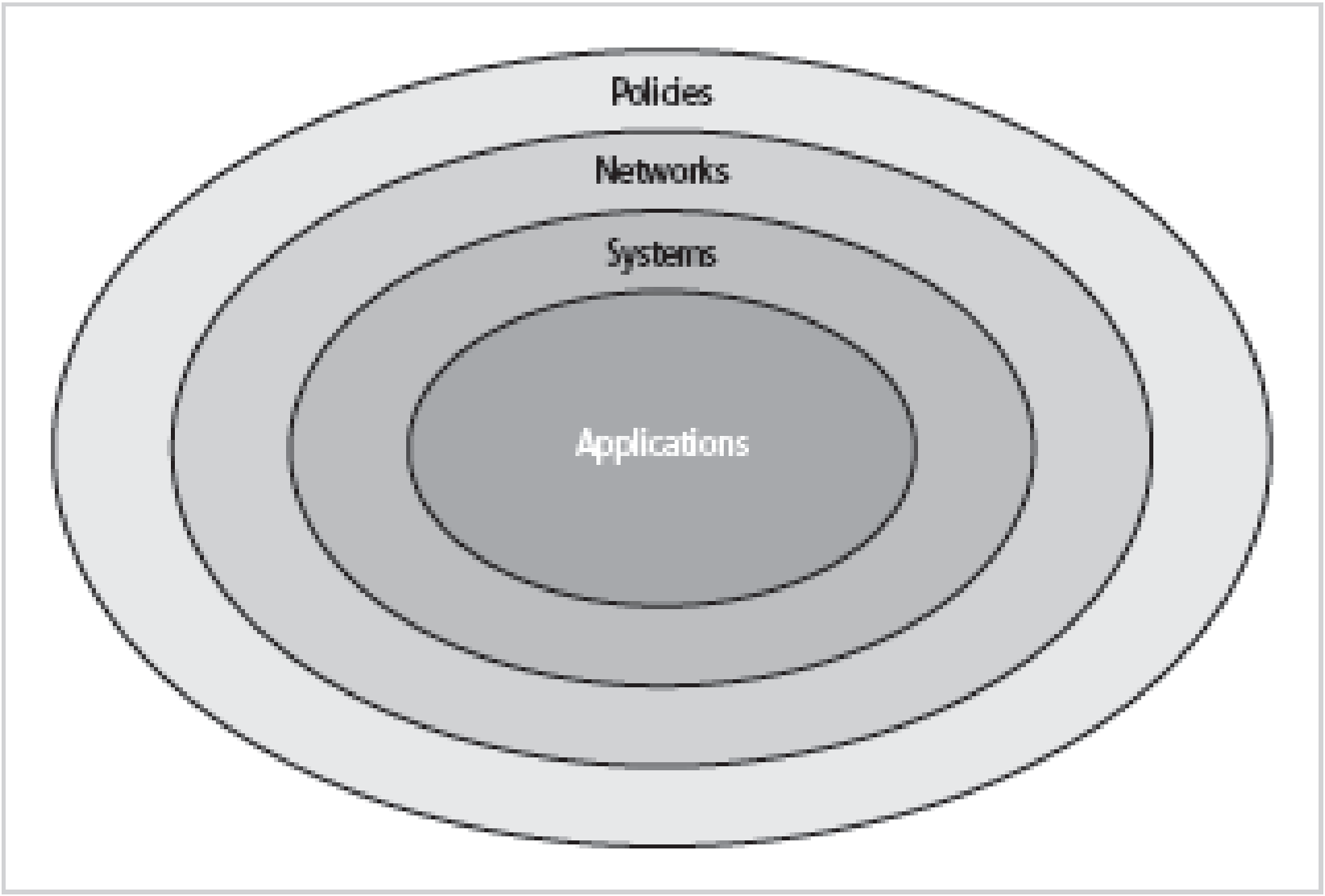

Figure 10-2 The Bull's-Eye Model

To Outsource or Not

- Just as some organizations outsource IT operations, organizations can outsource part or all of information security programs
- Due to complex nature of outsourcing, it's advisable to hire best outsourcing specialists and retain best attorneys possible to negotiate and verify legal and technical intricacies

Technology Governance and Change Control

- Technology governance
  - Complex process an organization uses to manage impact and costs from technology implementation, innovation, and obsolescence
- By managing the process of change, organization can:
  - Improve communication; enhance coordination; reduce unintended consequences; improve quality of service; and ensure groups are complying with policies

Nontechnical Aspects of Implementation

- Other parts of implementation process are not technical in nature, dealing with the human interface to technical systems
- Include creating a culture of change management as well as considerations for organizations facing change

The Culture of Change Management

- Prospect of change can cause employees to build up resistance to change
- The stress of change can increase the probability of mistakes or create vulnerabilities
- Resistance to change can be lowered by building resilience for change
- Lewin change model:
  - Unfreezing
  - Moving
  - Refreezing

Considerations for Organizational Change

- Steps can be taken to make organization more amenable to change:
  - Reducing resistance to change from beginning of planning process
  - Develop culture that supports change

Considerations for Organizational Change (cont'd.)

- Reducing resistance to change from the start
  - The more ingrained the previous 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: organization has come to expect change as a necessary part of organizational culture, and embracing change is more productive than fighting it
  - To develop such a culture, 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 the myriad of new federal regulation protecting personal privacy, organizations need to have some formal mechanism 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

Information Systems Security Certification and Accreditation (cont'd.)

- SP 800-37, Rev. 1: Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
  - Provides 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)

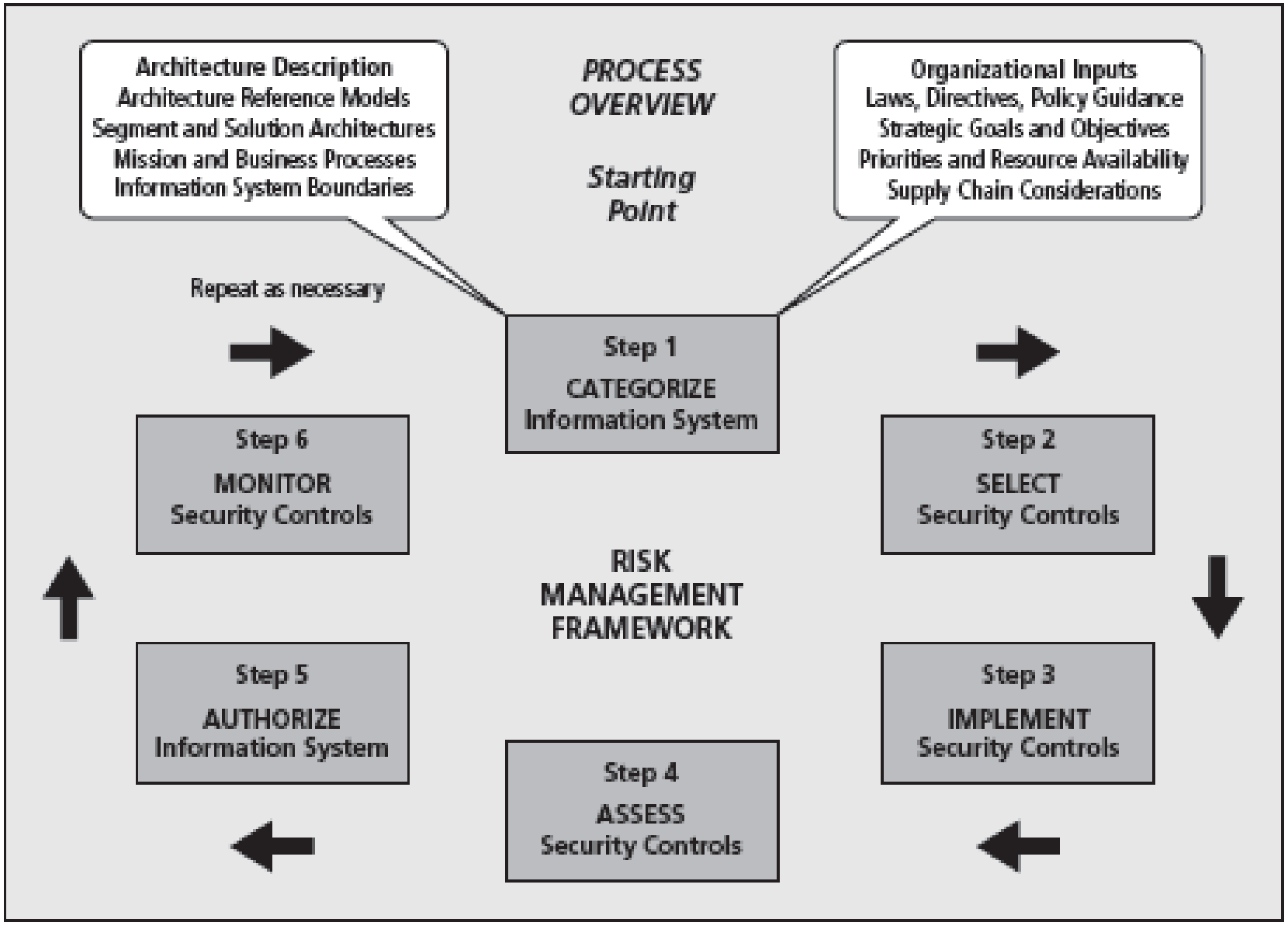

Figure 10-4 Risk Management Framework

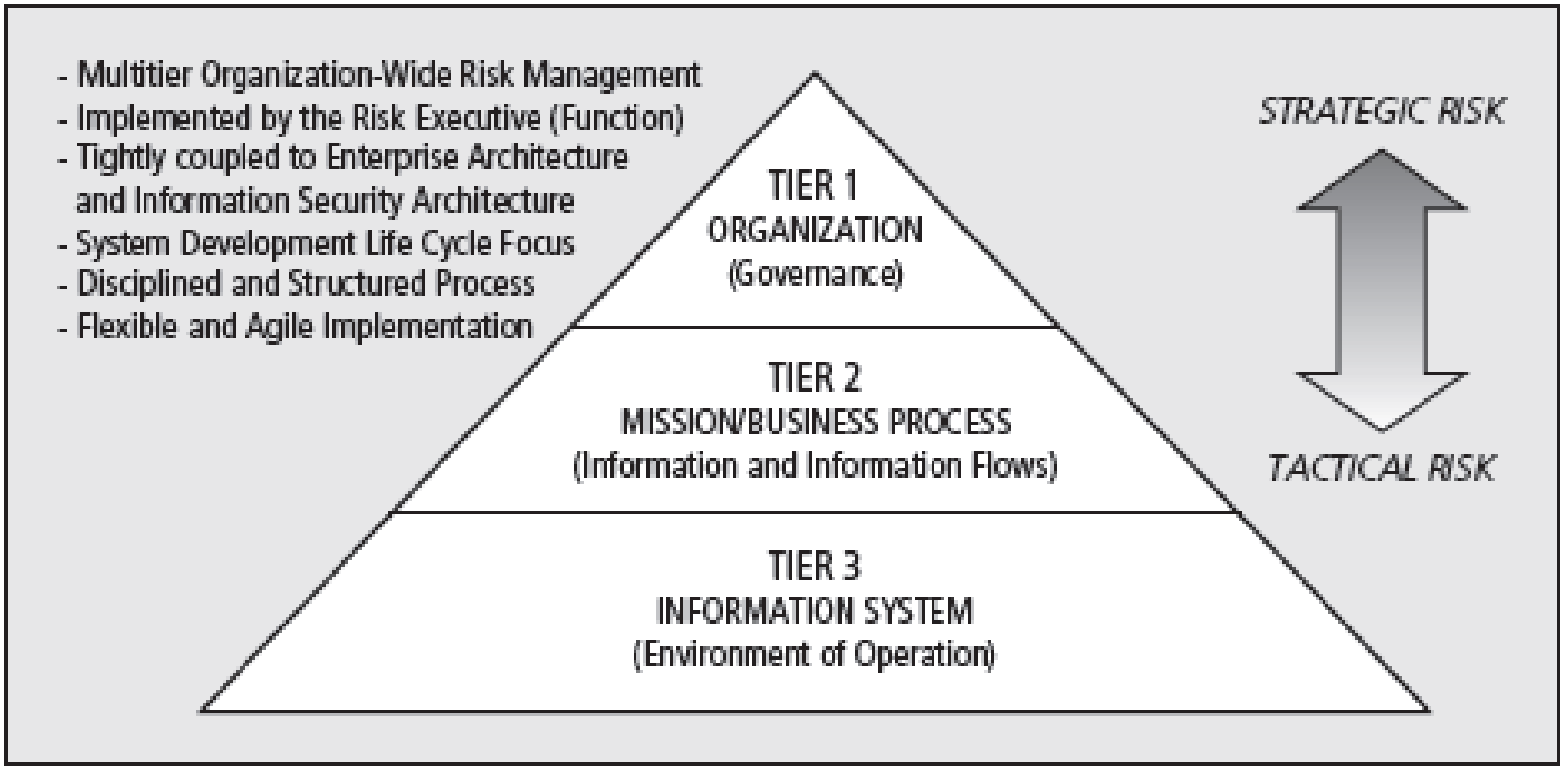

Figure 10-3 Tiered Risk Management Framework

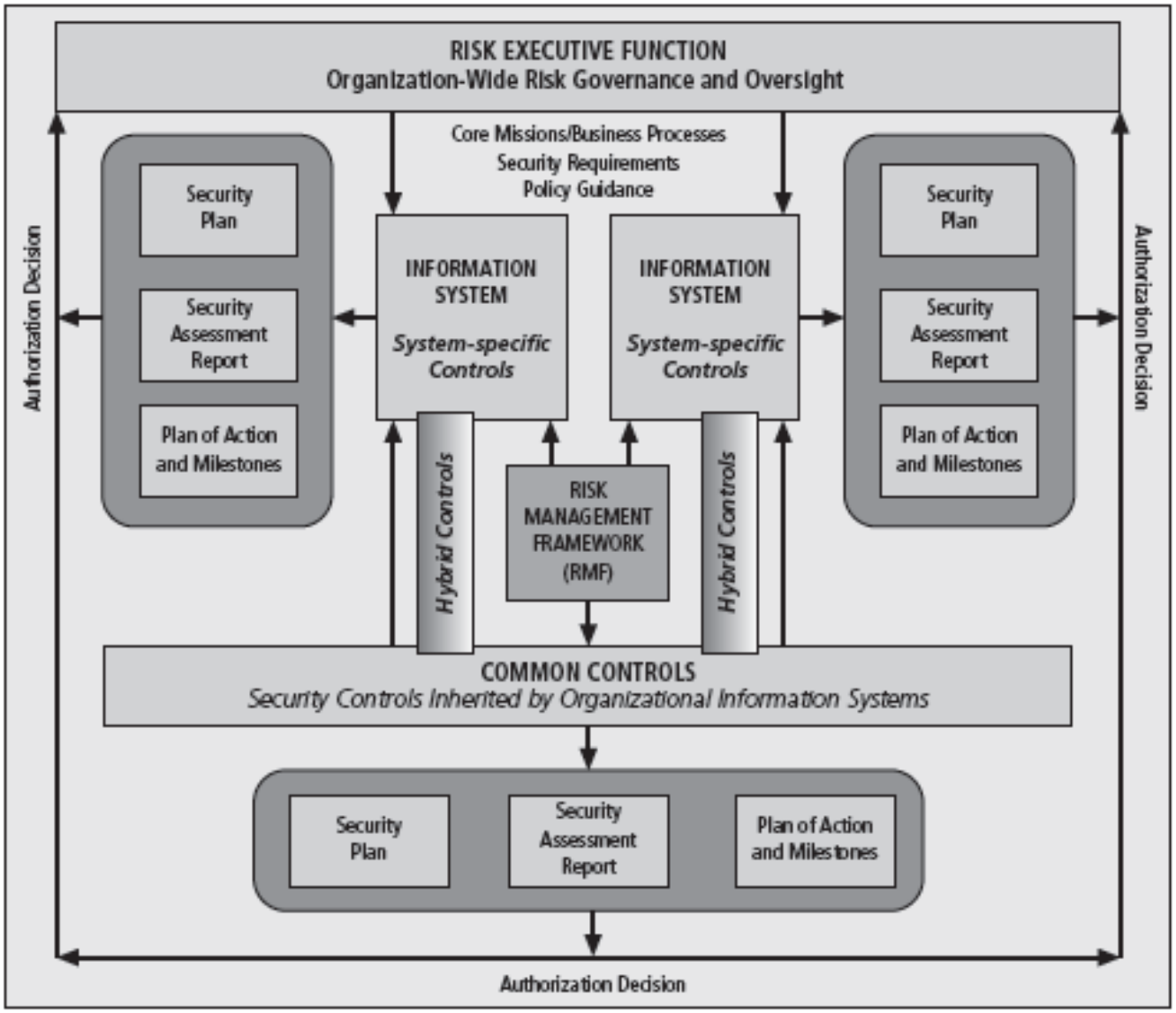

Figure 10-5 NIST SP 800-37, R.1: Security Control Allocation

Information Systems Security Certification and Accreditation (cont'd.)

- NSTISS Instruction-1000: National Information Assurance Certification and Accreditation Process (NIACAP)
  - The NIACAP is composed of four phases
    - Phase 1 – definition
    - Phase 2 – verification
    - Phase 3 – validation
    - Phase 4 – post accreditation

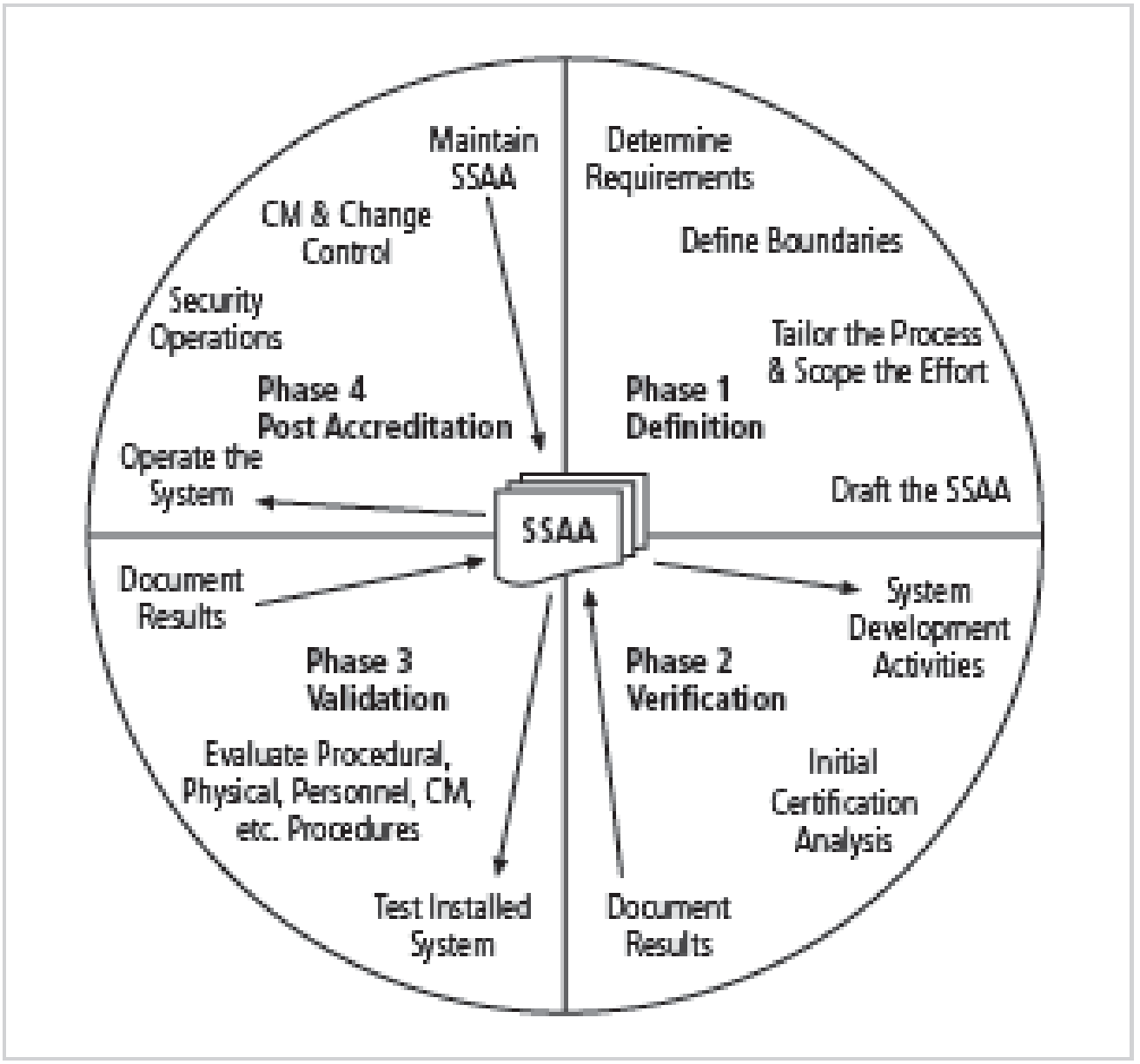

Figure 10-6 Overview of the NIACAP process

Information Systems Security Certification and Accreditation (cont'd.)

- ISO 27001/ 27002 Systems Certification and Accreditation
  - Entities outside the United States apply the standards provided under these standards
  - Standards were originally created to provide a foundation for British certification of information security management systems (ISMS)
  - Organizations wishing to demonstrate their systems have met this international standard must follow the certification process

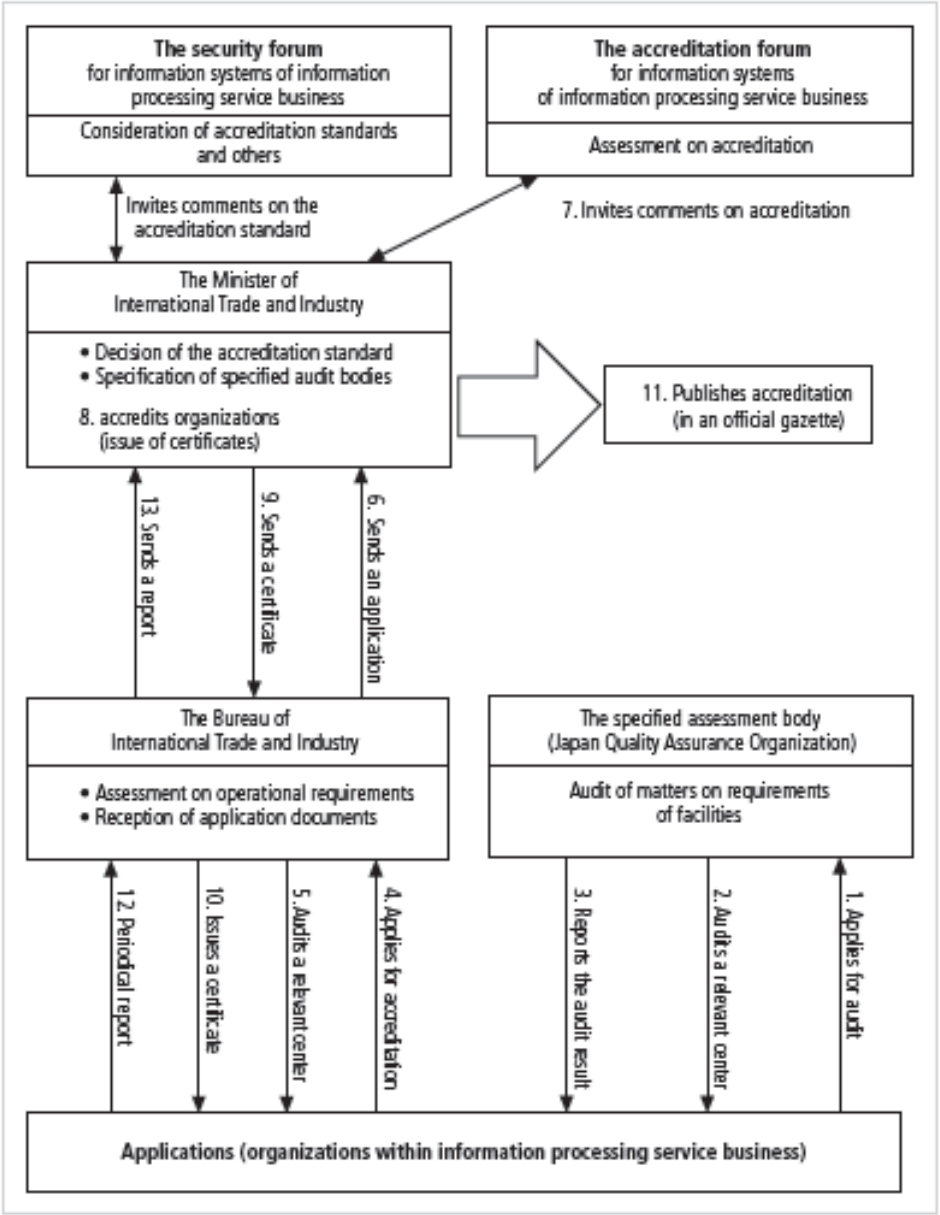

Figure 10-11 Japanese ISMS Certification and Accreditation

Summary

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