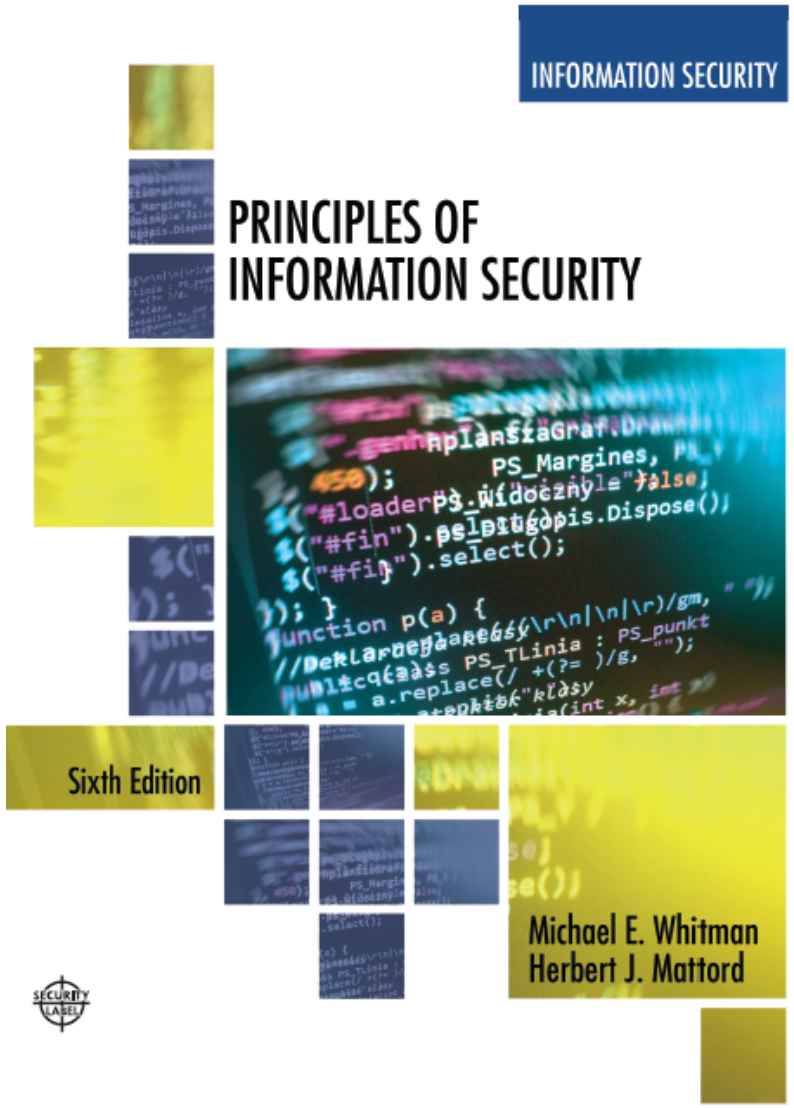


Source: Principles of Information Security

Chapter 10

Implementing Information Security

Dr. Ibrahim Waziri Jr.

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

Introduction

- InfoSec blueprint implementation 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 its 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 a tool such as the work breakdown structure (WBS).
- Major project tasks in WBS are:
  - Work to be accomplished (activities and deliverables)
  - The people or skill sets assigned to perform the task
  - Start and end dates for the task, when known
  - Amount of effort required for completion, in hours or work days
  - Estimated capital expenses for the task
  - Estimated noncapital expenses for the task
  - Identification of dependencies between and among tasks

Project Planning Considerations

Special considerations include financial, priority, time and schedule, staff, procurement, organizational feasibility, training and indoctrination, and scope.

Considerations:

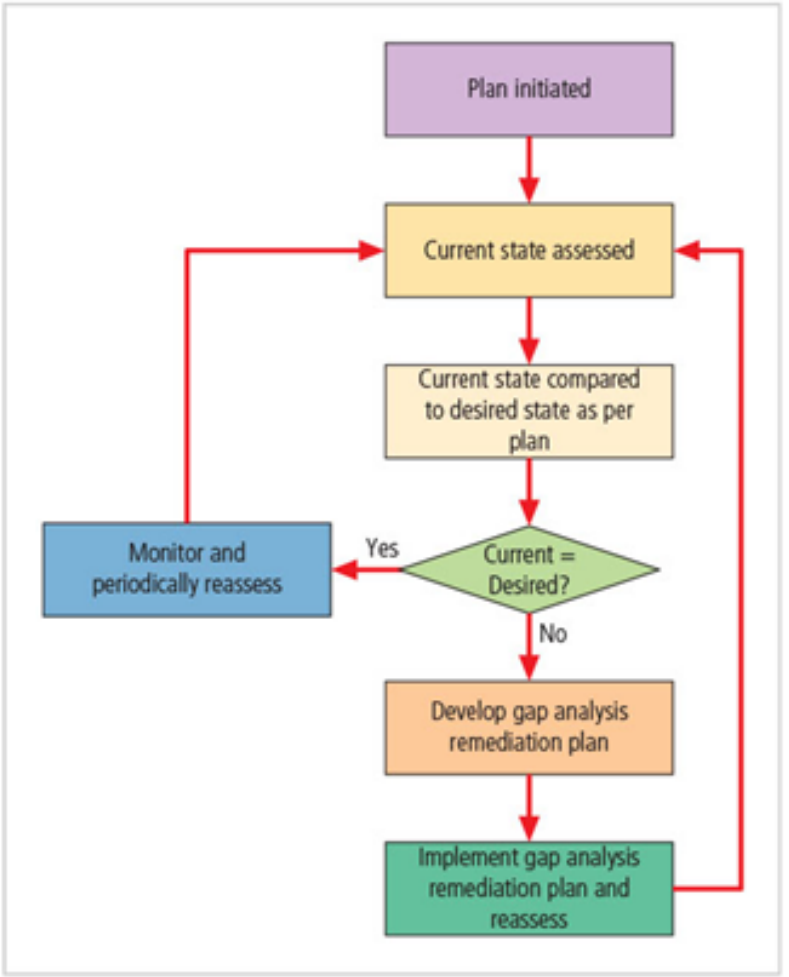
- Financial considerations
- Priority considerations
- Time and scheduling considerations
- Staffing considerations
- Procurement considerations
- Organizational feasibility considerations
- Training and indoctrination considerations
- Scope considerations

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.

- Supervised implementation
- Executing the plan
- Project wrap-up



Gap Analysis

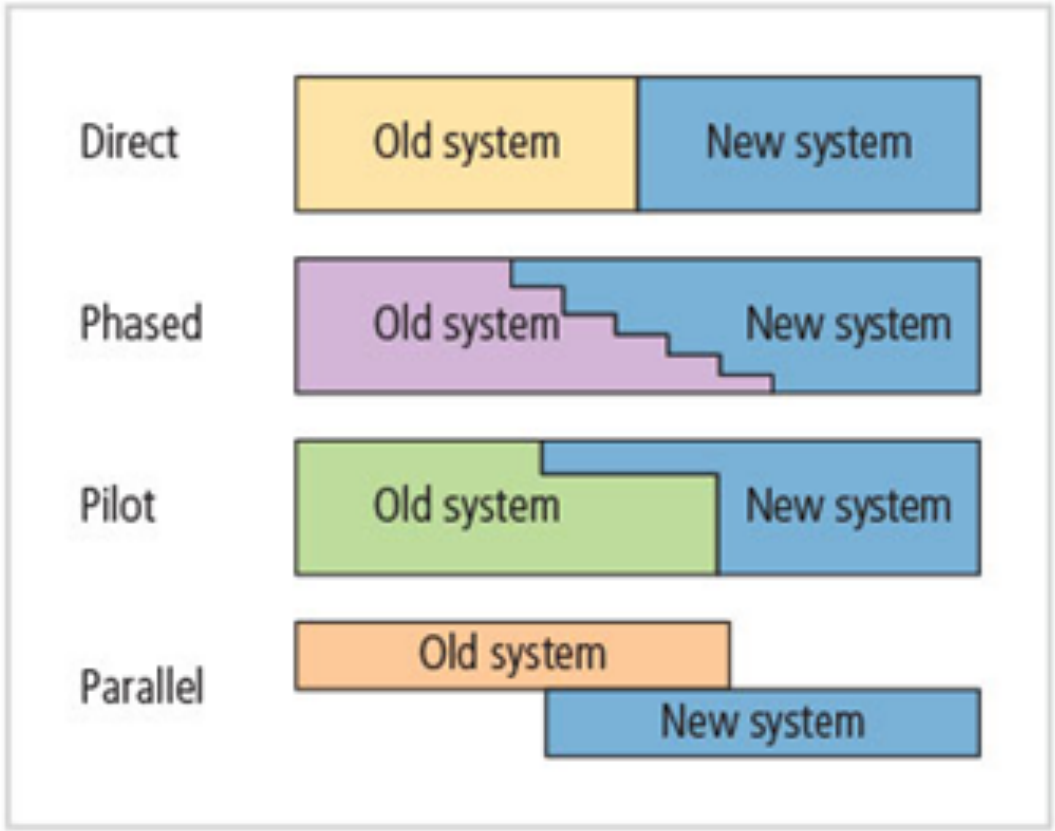
Security Project Management Certifications

- 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

Conversion Strategies

As the components of the new security system are planned, provisions must be made for changeover from the previous method of performing a task to the new method.

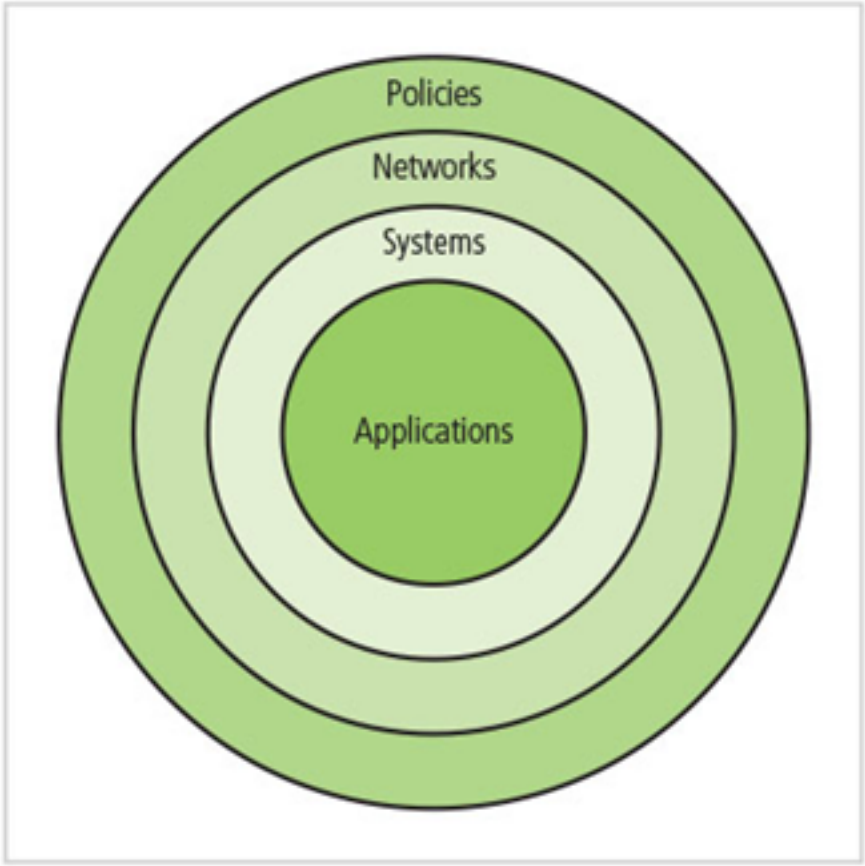
- Four basic approaches:
  - Direct changeover
  - Phased implementation
  - Pilot implementation
  - Parallel operations



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



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 the 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

Culture of Change Management & Considerations

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.

- 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

Information Systems Security Certification and Accreditation (C&A)

In order to comply with recent federal regulations protecting personal privacy, the organizations need to have formal mechanisms for verification and validation.

Accreditation: authorizes an 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.

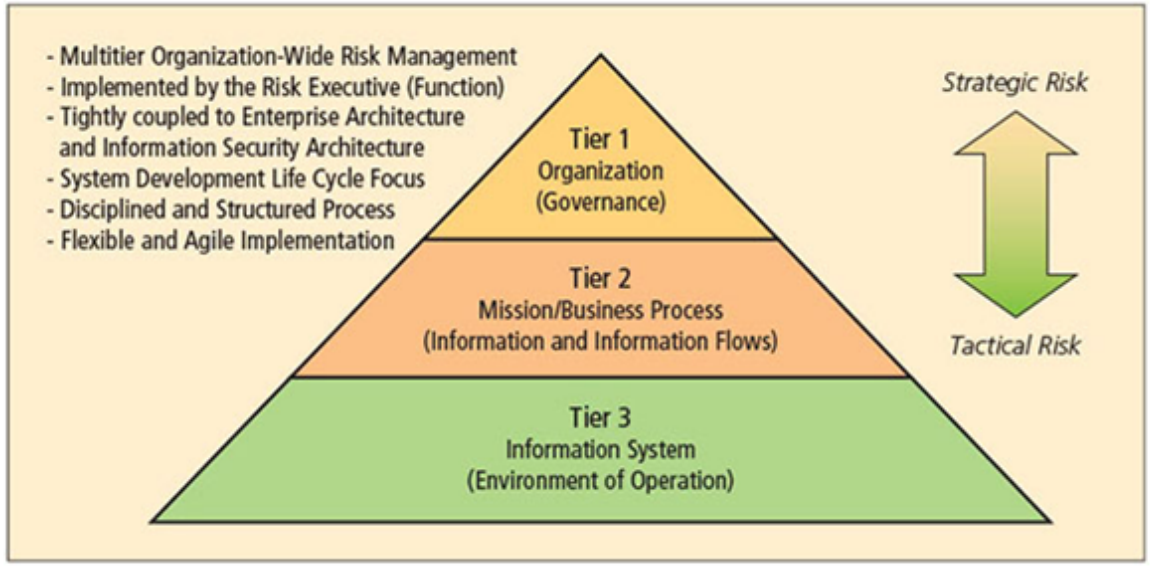
US Federal Systems - NIST Security Life Cycle

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 US federal government is grouped into one of three categories: National security information (NSI), Non-NSI, Intelligence community (IC).

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

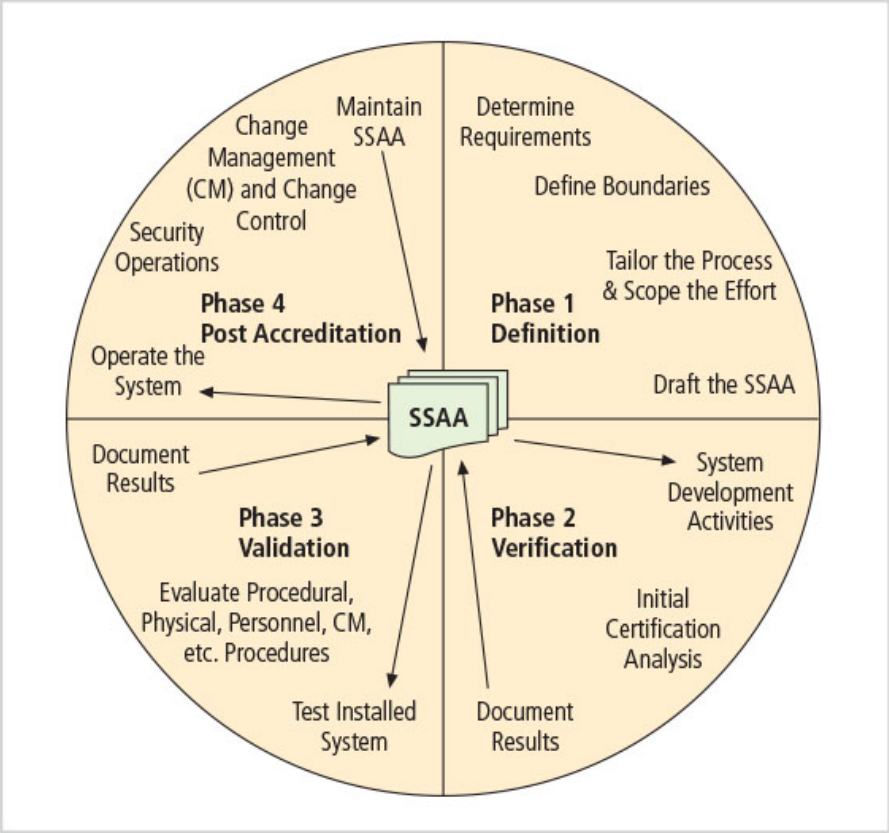
- Tier 1 addresses risk from organizational perspective
- Tier 2 addresses risk from mission/business process perspective
- Tier 3 addresses risk from information system perspective



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)

- Phase 1: Definition
- Phase 2: Verification
- Phase 3: Validation
- Phase 4: Post Accreditation



ISO 27001/ 27002 Systems C&A

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.

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