Management of Information Security, 4th Edition

Chapter 2

Planning for Security

Objectives

- Identify the roles in organizations that are active in the planning process
- Explain the principal components of information security (InfoSec) system implementation planning in the organizational planning scheme
- Differentiate between strategic organization InfoSec planning and specialized contingency planning (CP)
- List and explain the unique considerations and relationships that exist among the types of specialized CP-incident response, disaster recovery, and business continuity planning (BCP)

Introduction

- Planning is essential to business and organizational management
  - Good planning enables an organization to make the most out of the materials at hand
- Some organizations spend too much time, money, and human effort on planning with too little return to justify their investment
  - Each organization must balance the benefits of the chosen degree of planning effort against the costs of the effort

The Role of Planning

- Planning involves many interrelated groups and organizational processes
- Factors that can affect planning:
  - Physical environment
  - Political and legal environment
  - Competitive environment
  - Technological environment
- Stakeholders: people or organizations that have a “stake” in a particular aspect of the planning or operation of the organization
  - Often asked for input on strategic decisions

The Role of Planning (continued)

- Planning is the dominant means of managing resources in modern organizations
  - Provides direction for the organization's future
- Without specific and detailed planning:
  - Organizational units would attempt to meet objectives independently and will result in inefficient use of resources
- Primary goal of organizational planning is the creation of detailed plans

Precursors to Planning

- To implement effective planning:
  - Organization's leaders usually begin from previously developed positions that state the organization's ethical, entrepreneurial, and philosophical perspectives
- When an organization's stated positions do not match the demonstrated ethical, entrepreneurial, and philosophical approaches of its management teams:
  - The developmental plan becomes unmanageable

Values Statement

- Values statement should be one of the first positions that management must articulate
  - The trust and confidence of stakeholders and the public are important
- By establishing a formal set of principles and qualities in a values statement:
  - An organization makes its conduct and performance standards clear to its employees and the public

Figure 2-2 Microsoft's mission and values statement

Source: Microsoft.

Vision Statement

- The vision statement expresses what the organization wants to become
  - Should be ambitious
  - It is the best-case scenario for the organization's future
  - Not meant to express the probably, only the possible
- Many organization's mix or combine the vision statement and the mission statement

Mission Statement

- The mission statement explicitly declares the business of the organization and its intended areas of operation
- A mission statement should:
  - Be concise
  - Reflect both internal and external operations
  - Be robust enough to remain valid for a period of four to six years
- Many organizations encourage each division or major department to generate its own mission statement

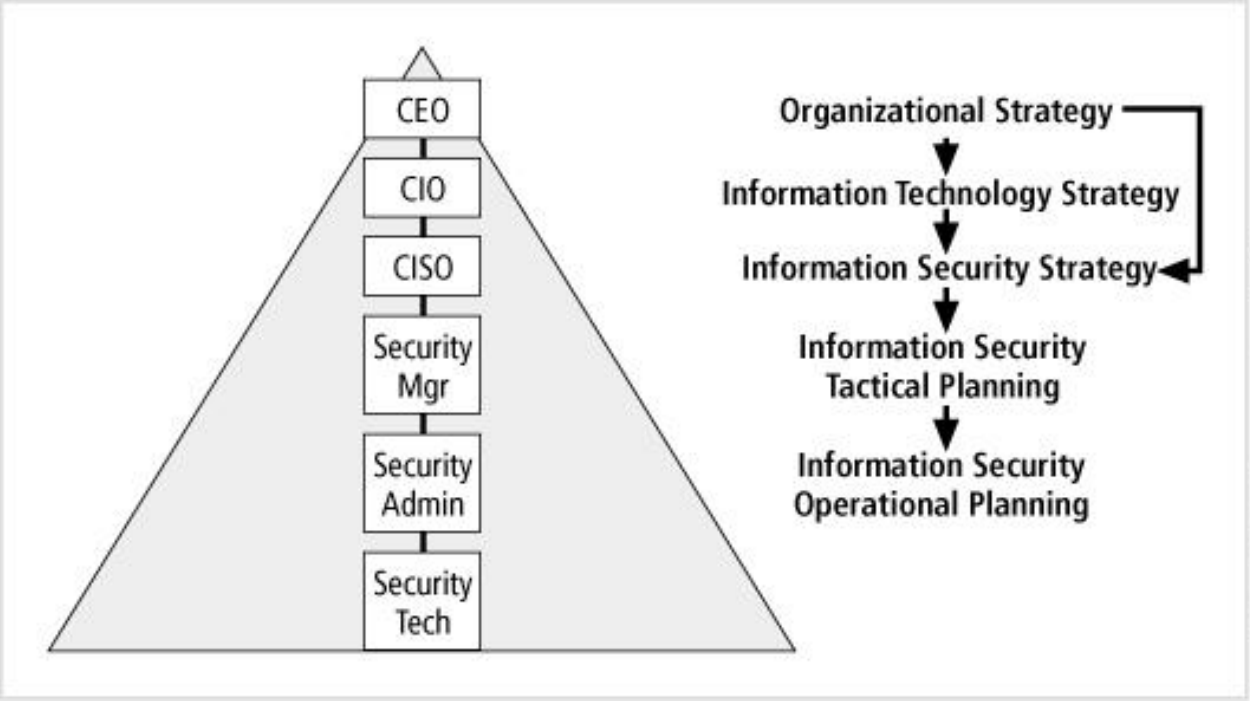
Mission Statement (continued)

- Mission statement is the follow-up to the vision statement
  - The vision statement states where the organization wants to go and the mission statement describes how it wants to get there
- Together, the mission, vision, and values statements provide the philosophical foundation for planning
  - They guide the creation of the strategic plan

Strategic Planning

- **Strategic planning:** lays out the long-term direction to be taken by the organization
  - Guides organizational efforts and focuses resources toward specific, clearly defined goals in the midst of an ever-changing environment
- Strategic plans formed at the highest levels of the organization are translated into more specific strategic plans for intermediate layers of management

Figure 2-3 Top-down strategic planning



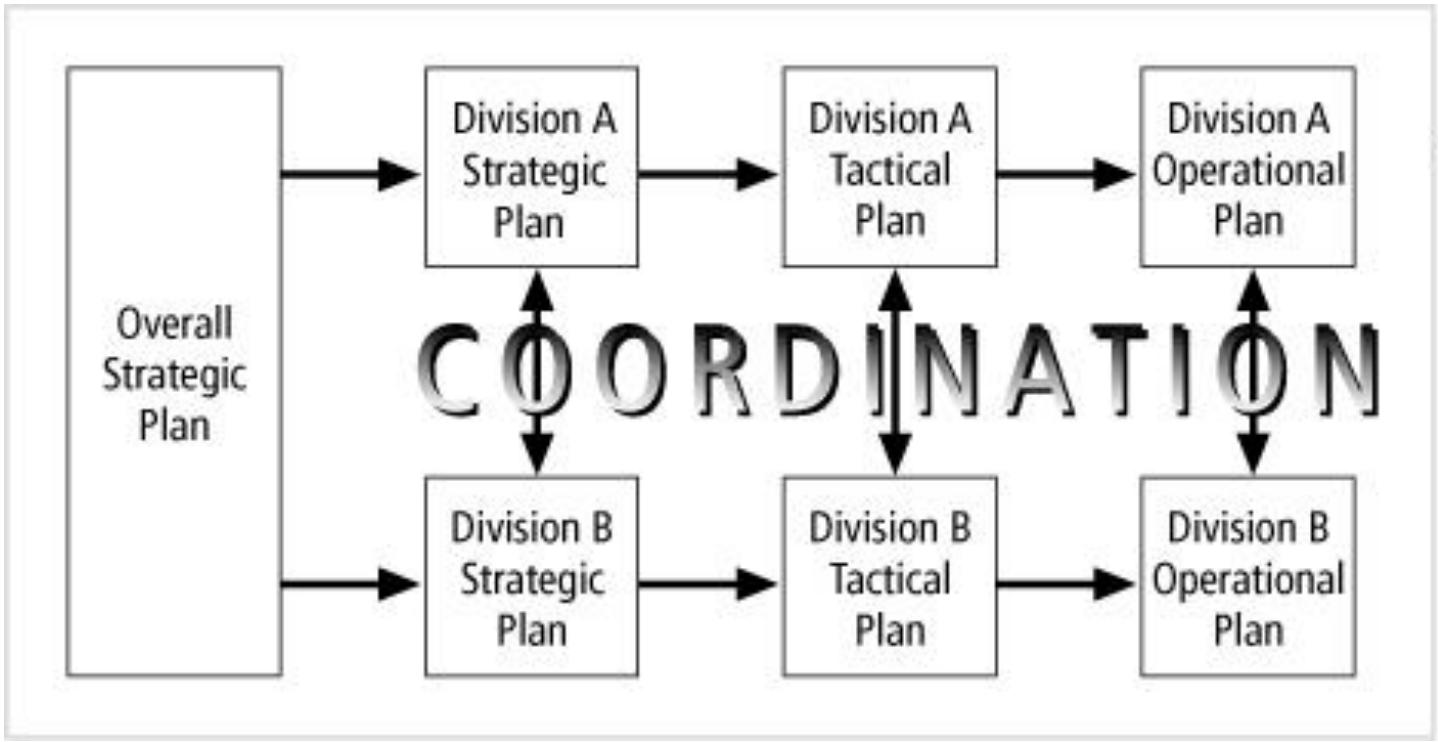
Creating a Strategic Plan

- Organization's must create an overall strategic plan by extending the general strategy into specific strategic plans for major divisions
  - Each level of each division translates objectives into more specific objectives for the level below
- The conversion of goals from the strategic level to the next lower level

Planning Levels Part 1

- Once strategic goals for each major division have been identified:
  - The next step is to translate these strategies into tasks with specific, measurable, achievable, and time-bound objectives
- Strategic planning transforms general, sweeping statements toward specific and applied objectives

Figure 2-4 Strategic planning levels



Planning Levels Part 2

- Tactical planning has a more short-term focus than strategic planning
- Budgeting, resource allocation, and personnel are critical components of the tactical plan
- Tactical plans are often created for specific projects
  - Some organizations call this process project planning or intermediate planning

Planning Levels Part 3

- Managers and employees use operational plans to organize the ongoing, day-to-day performance tasks
- Operational planning within InfoSec may encompass such objectives as:
  - The selection, configuration, and deployment of a firewall
  - The design and implementation of a security education, training, and awareness (SETA) program

Planning and the CISO

- The first priority of the CISO and InfoSec team should be the structure of a strategic plan
- The basic components of a typical strategic plan:
  - Executive Summary
  - Mission and Vision Statement
  - Organizational Profile and History
  - Strategic Issues and Core Values
  - Program Goals and Objectives
  - Management/Operations Goals and Objectives
  - Appendices (optional)

Information Security Governance

- **Governance, risk management, and compliance (GRC):** seeks to integrate these three responsibilities into one holistic approach that can provide sound executive-level strategic planning and management of the InfoSec function
- InfoSec objectives must be addressed at the highest levels of an organization's management team
  - In order to be effective and offer a sustainable approach

Information Security Governance (continued)

- According to the Information Technology Governance Institute (ITGI):
  - InfoSec governance includes all the accountabilities and methods undertaken by the board of directors and executive management to provide:
    - Strategic direction
    - Establishment of objectives
    - Measurement of progress toward objectives
    - Verification that risk management practices are appropriate
    - Validation that assets are used properly

Desired Outcomes

- Five basic outcomes of InfoSec governance:
  - Strategic alignment of InfoSec with business strategy to support organizational objectives
  - Risk management by executing appropriate measures to manage and mitigate threats to information resources
  - Resource management by utilizing InfoSec knowledge and infrastructure efficiently and effectively

Desired Outcomes (continued)

- Five basic outcomes of InfoSec governance (cont'd):
  - Performance measurement by measuring, monitoring, and reporting InfoSec governance metrics to ensure organizational objectives are achieved
  - Value delivery by optimizing InfoSec investments in support of organizational objectives

Benefits of Information Security Governance

- Benefits, if properly implemented, include:
  - An increase in share value for organizations
  - Increased predictability and reduced uncertainty of business operations
  - Protection from increasing potential for civil or legal liability
  - Optimization of the allocation of limited security resources
  - Assurance of effective InfoSec policy and policy compliance

Benefits of Information Security Governance (continued)

- Benefits (cont'd):
  - A firm foundation for efficient and effective risk management, process improvement, and rapid incident response
  - A level of assurance that critical decisions are not based on faulty information
  - Accountability for safeguarding information during critical business activities
    - Such as mergers and acquisitions, business process recovery, and regulatory response

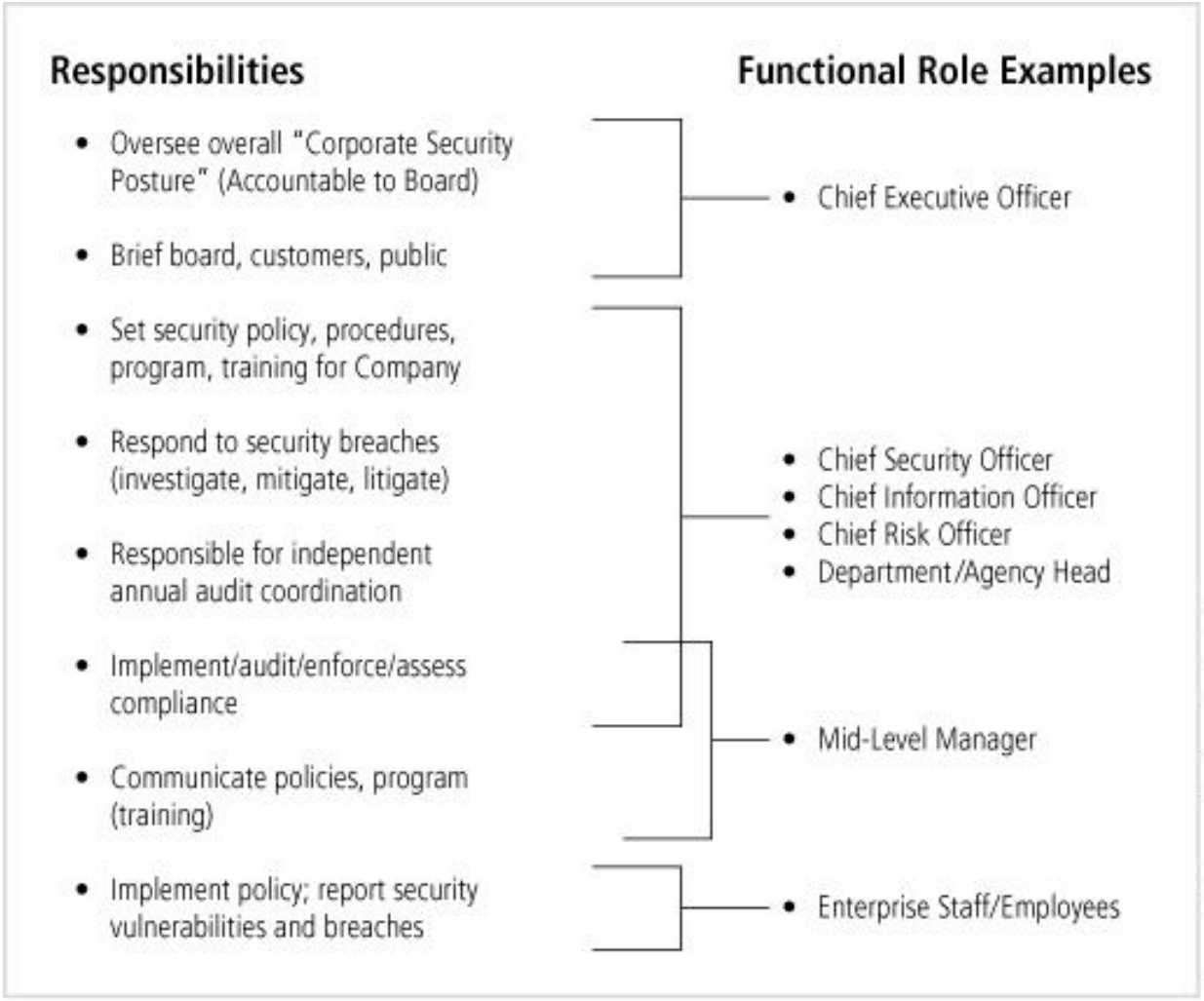
Implementing Information Security Governance

- Core set of activities:
  - Conduct an annual InfoSec evaluation, reviewed by CEO and reported to the board of directors
  - Conduct periodic risk assessments of information assets
  - Implement policies and procedures based on risk assessments to secure information assets
  - Establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability
  - Develop plans and initiate actions to provide for adequate InfoSec

Implementing Information Security Governance (continued)

- Core set of activities (cont'd):
  - Treat InfoSec as an integral part of the system
  - Provide InfoSec awareness, training, and education
  - Conduct periodic testing and evaluation of the effectiveness of InfoSec policies and procedures
  - Create and execute a plan for remedial action to address any InfoSec deficiencies
  - Develop and implement incident response procedures
  - Establish plans, procedures, and tests to provide continuity of operations
  - Use security best practices guidance

Figure 2-7 Information security governance responsibilities



Security Convergence

- Enterprise risk management (ERM): approach that can gain superior alignment of security functions with the business mission while lowering costs
- Key approaches to achieve unified ERM:
  - Combining physical security and InfoSec under one leader as a business function
  - Using separate business functions that report to a common senior executive
  - Using a risk council approach to provide a collaborative approach to risk management
    - Representatives from across the organization

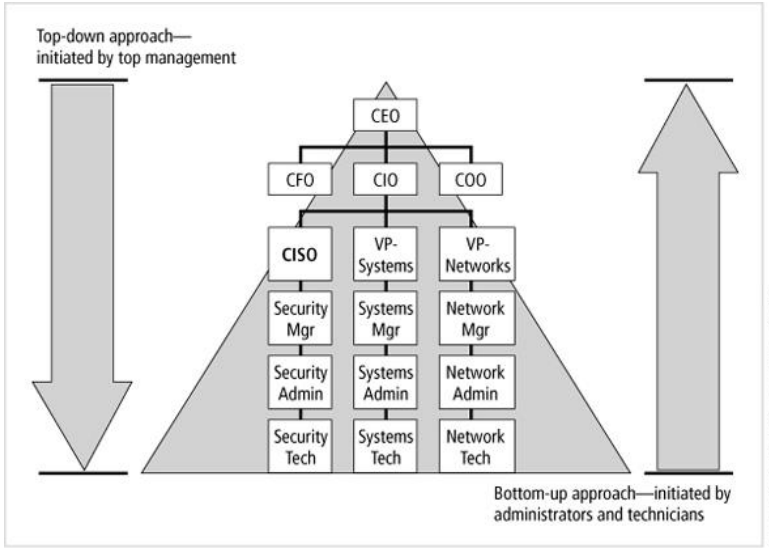
Planning for Information Security Implementation Part 1

- CIO and CISO play important roles in translating overall strategic planning into tactical and operational InfoSec plans
- Depending on the InfoSec function's placement within the organizational chart:
  - The CISO may report directly to the CIO
- CISO plays a more active role in the development of the planning details than the CIO

Planning for Information Security Implementation Part 2

- Implementation of InfoSec can occur in two ways:
  - Bottom-up approach - initiated by administrators and technicians
  - Top-down approach - initiated by top management

Figure 2-8 Approaches to security implementation



Planning for Information Security Implementation Part 3

- For top-down approach to succeed:
  - High-level management must buy into the effort and provide full support to all departments
  - Must have a **champion**-an executive with sufficient influence to move the project forward
- Involvement and support of end users is critical
  - Key end users should be assigned to design teams, known as **joint application design teams (JADs)**
  - A successful JAD must be able to survive employee turnover

Planning for Information Security Implementation Part 4

- Key steps to ensure the JAD approach succeeds:
  - Identify project objectives and limitations
  - Identify critical success factors
  - Define project deliverables
  - Define the schedule of workshop activities
  - Select participants
  - Prepare the workshop material
  - Organize workshop activities and exercises
  - Prepare, inform, and educate workshop participants
  - Coordinate workshop logistics

Introduction to the Security Systems Development Life Cycle

- Security Systems Development Life Cycle (SecSDLC): a methodology for the design and implementation of an information system in an organization
  - **Methodology**: a formal approach to solving a problem based on a structured sequence of procedures
- Using a methodology ensures a rigorous process and increases the likelihood of achieving the desired final objective

Introduction to the Security Systems Development Life Cycle (continued)

- The driving force to begin an SDLC-based project may be:
  - **Event-driven**: a response to some event in the business community, inside the organization, or within the ranks of employees, customers, or other stakeholders
  - **Plan-driven**: the result of a carefully developed planning strategy
- At the end of each phase, a **structured review** (reality check) takes place
  - To decide if project should be continued, outsourced, or postponed

Investigation in the SecSDLC

- Investigation phase begins with a directive from upper management
  - Specifying the process, outcomes, and goals of the project as well as budget and other constraints
- Teams of managers, employees, consultants are assembled to:
  - Investigate problems
  - Define their scope
  - Specify goals and objectives
  - Identify any additional constraints not covered in the enterprise security policy

Analysis in the SecSDLC Part 1

- In the analysis phase, the team studies documents from the investigation phase
  - Also includes an analysis of relevant legal issues that could affect the design of the security solution
  - Risk management begins - which is the process of identifying, assessing, and evaluating the levels of risk
- Threat: an object, person, or other entity that represents a constant danger to an asset
- There are 12 general categories that represent real and present dangers to information systems

Table 2-1 Threats to information security

Threat	Description/Example
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc
Human error or failure	Accidents, employee mistakes, failure to follow policy
information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial-of-services. or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, back doors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Analysis in the SecSDLC Part 2

- Theft poses a huge threat to an organization's information systems
- **Attack**: an act or event that exploits a vulnerability
- **Vulnerability**: an identified weakness of a controlled information asset
  - Is the result of absent or inadequate controls
- **Threat agent**: accomplishes an attack by damaging or stealing an organization's information or physical assets
- **Exploit**: a technique or mechanism used to compromise an information asset

Analysis in the SecSDLC Part 3

- Once threats have been identified, an organization should assess the risk for each of the information assets via a process called **risk assessment or risk analysis**
  - Both are components of risk management
- **Risk management**: part of the analysis phase that identifies vulnerabilities in an organization's information systems
  - Must take steps to assure confidentiality, integrity, and availability of information systems
- **Risk assessment**: assigns a comparative risk rating or score to each specific information asset

Design in the SecSDLC Part 1

- Design phase consists of two distinct phases:
  - Logical design - team members create and develop the blueprint for security
    - Examine and implement key policies that influence later decisions
    - Contingency plans for incident response are developed
  - Physical design - team members evaluate the technology needed to support the security blueprint, generate alternative solutions, and agree on a final design
    - A feasibility study should determine readiness for proposed project

Design in the SecSDLC Part 2

- Information security policy (InfoSec policy): provides rules for the protection of information assets
- Along with application of the security policy
  - Education and training programs should be offered to organization members
- The design phase includes the formulation of controls and safeguards used to protect information
  - The terms **control** and **safeguard** are often used
- There are three categories of controls: managerial controls, operational controls, and technical controls

Design in the SecSDLC Part 3

- **Managerial controls**: cover security processes that are designed by the strategic planners and executed by the security administration of the organization
  - Set the direction and scope of the security process
- **Operational controls**: deal with the operational functionality of security in the organization
  - Cover management functions and lower-level planning
- **Technical controls**: address technical approaches used to implement security
  - Must be integrated into the IT structure

Design in the SecSDLC Part 4

- Contingency plans (CP) - the overall planning to prepare for, react to, and recover from events that threaten security of information assets in the organization
- DRP - the planning process associated with the preparation for and recovery from a disaster
- IRP - the planning process associated with the identification, classification, response, and recovery from an incident
- BCP - the planning process associated with ensuring that critical business functions continue if a catastrophic incident or disaster occurs

Implementation in the SecSDLC Part 1

- During the implementation phase:
  - Security solutions are acquired, tested, implemented, and retested
  - Personnel issues are evaluated
  - Specific training and education programs are conducted
  - Entire tested package is presented to upper management for final approval
- An important element of this phase is the management of the project plan

Implementation in the SecSDLC Part 2

- Execution of the project plan occurs in three steps:
  - Planning the project
  - Supervising the tasks and action steps within the project plan
  - Wrapping up the project plan
- Roles of the development team:
  - *Champion*
  - *Team leader*
  - *Security policy developers*
  - *Risk assessment specialists*

Implementation in the SecSDLC Part 3

- Roles of the development team (cont'd):
  - *Security professionals*
  - *Systems administrators*
  - *End users*
- When implementing InfoSec in an organization:
  - Decide how to position and name the security function
  - Plan for proper staffing for the InfoSec function
  - Understand how InfoSec affects every role in IT
  - Integrate solid InfoSec concepts into personnel management practices

Implementation in the SecSDLC Part 4

- Various roles involved in InfoSec:
  - Chief information officer (CIO)
  - Chief security officer (CSO)
  - Chief information security officer (CISO)
  - Security managers
  - Security technicians
  - Data owners
  - Data custodians
  - Data users

Maintenance in the SecSDLC Part 1

- InfoSec systems need constant monitoring, testing, modifying, updating, and repairing
- Once the InfoSec program is implemented
  - It must be operated, properly managed, and kept up-to-date by means of established procedures
- As deficiencies are found and vulnerabilities pinpointed
  - Projects to maintain, extend, or enhance the program follow the SecSDLC steps

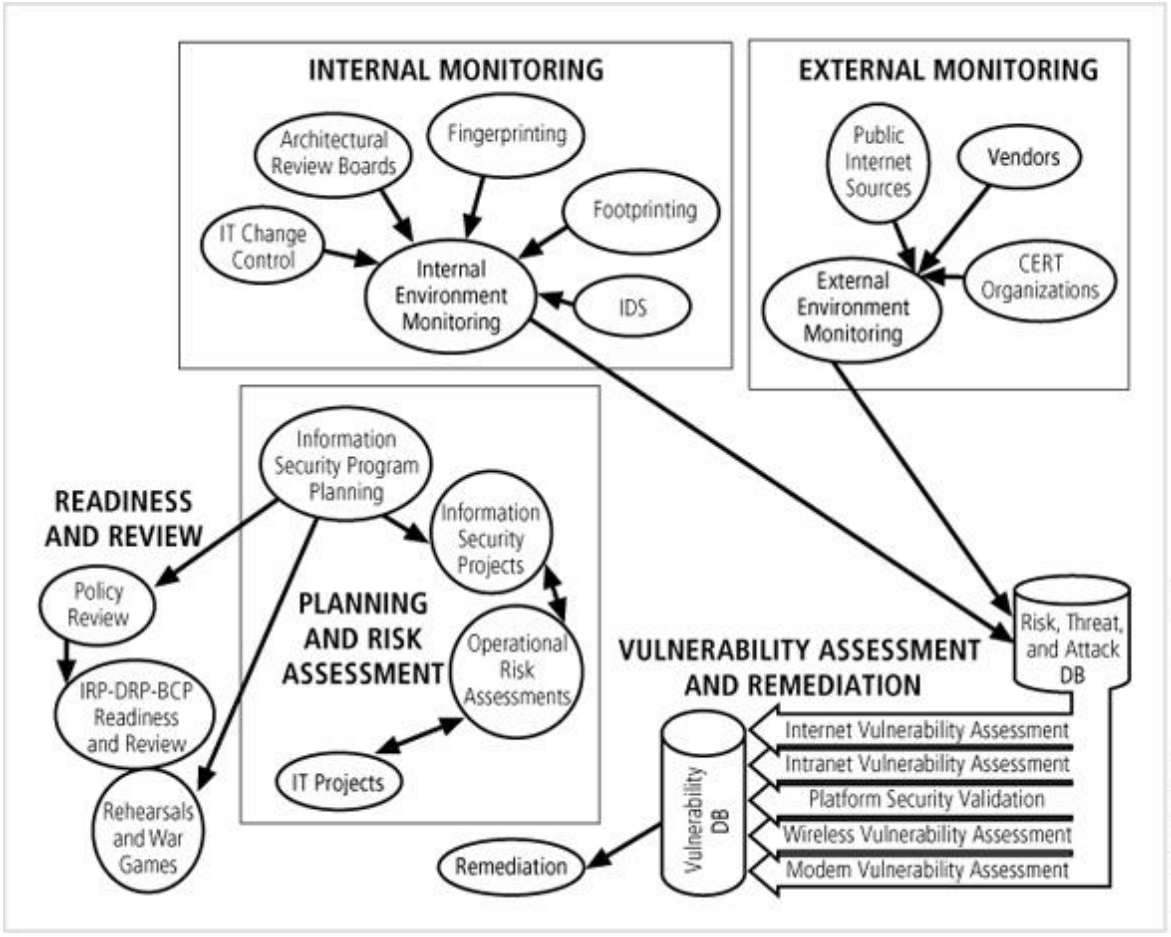
Maintenance in the SecSDLC Part 2

- A maintenance model is intended to focus ongoing maintenance efforts that are needed to keep systems useable and secure
- A maintenance model consists of five subject areas or domains:
  - **External monitoring**: to provide early awareness of new and emerging threats, threat agents, vulnerabilities, and attacks
  - **Internal monitoring**: to maintain an informed awareness of the state of all organization's networks, information systems, and InfoSec defenses

Maintenance in the SecSDLC Part 3

- A maintenance model consists of five subject areas or domains (cont'd):
  - **Planning and Risk Assessment**: to keep a wary eye on the entire InfoSec program
  - **Vulnerability Assessment and Remediation**: the identification of specific, documented vulnerabilities and their timely remediation
    - **Penetration testing**: to perform controlled attacks by exploiting documented vulnerabilities
  - **Readiness and Review**: to keep the InfoSec program functioning as designed and continuously improve it

Figure 2-10 Maintenance model



Summary Part 1

- Planning is central to the management of any organization and is based on the preparation, application, and control of a sequence of action steps to achieve specific goals
- To develop and implement effective planning, documents, documents representing the philosophical, ethical, and entrepreneurial perspectives of the company are first created
- Security can begin either as a grass-roots effort or with plans formulated by senior management

Summary Part 2

- The systems development life cycle (SDLC) is a methodology for the design and implementation of an information system in an organization
- The investigation phase of the SecSDLC begins with a directive from upper management dictating the process, outcomes, and goals of the project
- In the analysis phase, the team examines existing security policies along with documented current threats and associated controls
- The design phase includes two distinct phases: the logical design and the physical design

Summary Part 3

- The maintenance and change phase, though last, is perhaps the most important, given the flexibility and persistence of many of the threats facing the modern organization