



TEL2813/IS2820

Security Management

Security Planning

Lecture 2

Jan 22, 2008



Security Planning



Introduction

- Successful organizations utilize planning
- Planning involves:
 - Employees
 - Management
 - Stockholders
 - Other outside stakeholders
 - Physical environment
 - Political and legal environment
 - Competitive environment
 - Technological environment



Introduction

- Planning:
 - Is creating action steps toward goals, and then controlling them
 - Provides direction for the organization's future
- Top-down method:
 - Organization's leaders choose the direction
 - Planning begins with the general and ends with the specific



Introduction

- Strategic planning includes:
 - Vision statement
 - Mission statement
 - Strategy
 - Coordinated plans for sub units
- Knowing how the general organizational planning process works helps in the information security planning process

Information Security Planning

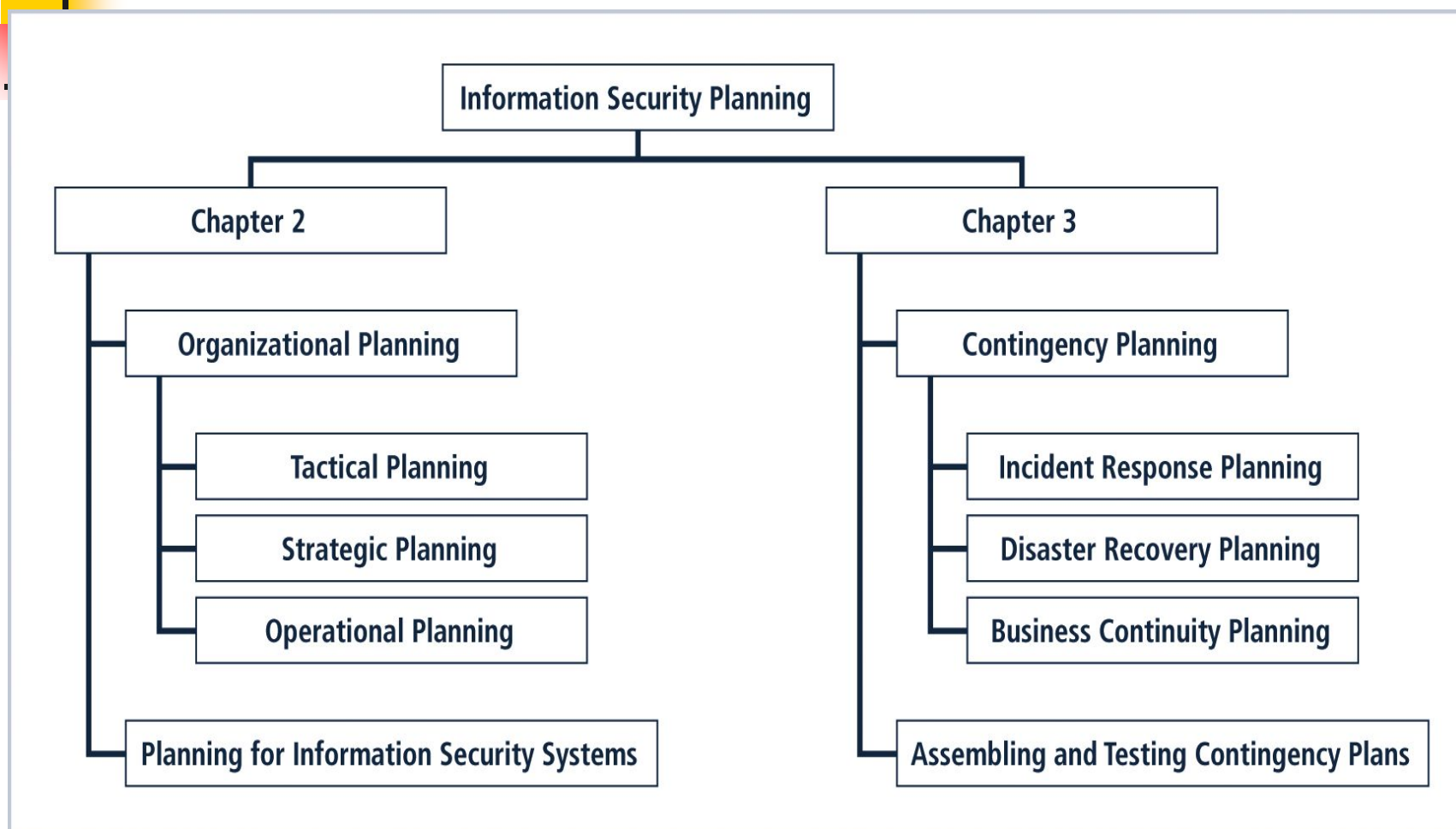


FIGURE 2-1 Information Security Planning



Components Of Planning: Mission Statement

- Mission statement:
 - Declares the business of the organization and its intended areas of operations
 - Explains what the organization does and for whom
 - Example:
 - Random Widget Works, Inc. designs and manufactures quality widgets, associated equipment and supplies for use in modern business environments



Components Of Planning: Vision Statement

- Vision statement:
 - Expresses what the organization wants to become
 - Should be ambitious
 - Example:
 - Random Widget Works will be the preferred manufacturer of choice for every business's widget equipment needs, with an RWW widget in every machine they use



Components Of Planning: Values

- By establishing organizational principles in a values statement, an organization makes its conduct standards clear
 - Example:
 - RWW values commitment, honesty, integrity and social responsibility among its employees, and is committed to providing its services in harmony with its corporate, social, legal and natural environments.
- The mission, vision, and values statements together provide the foundation for planning



Components Of Planning: Strategy

- Strategy is the basis for long-term direction
- Strategic planning:
 - Guides organizational efforts
 - Focuses resources on clearly defined goals

“... strategic planning is a disciplined effort to produce fundamental decisions and actions that shape and guide what an organization is, what it does, and why it does it, with a focus on the future.”

Strategic Planning

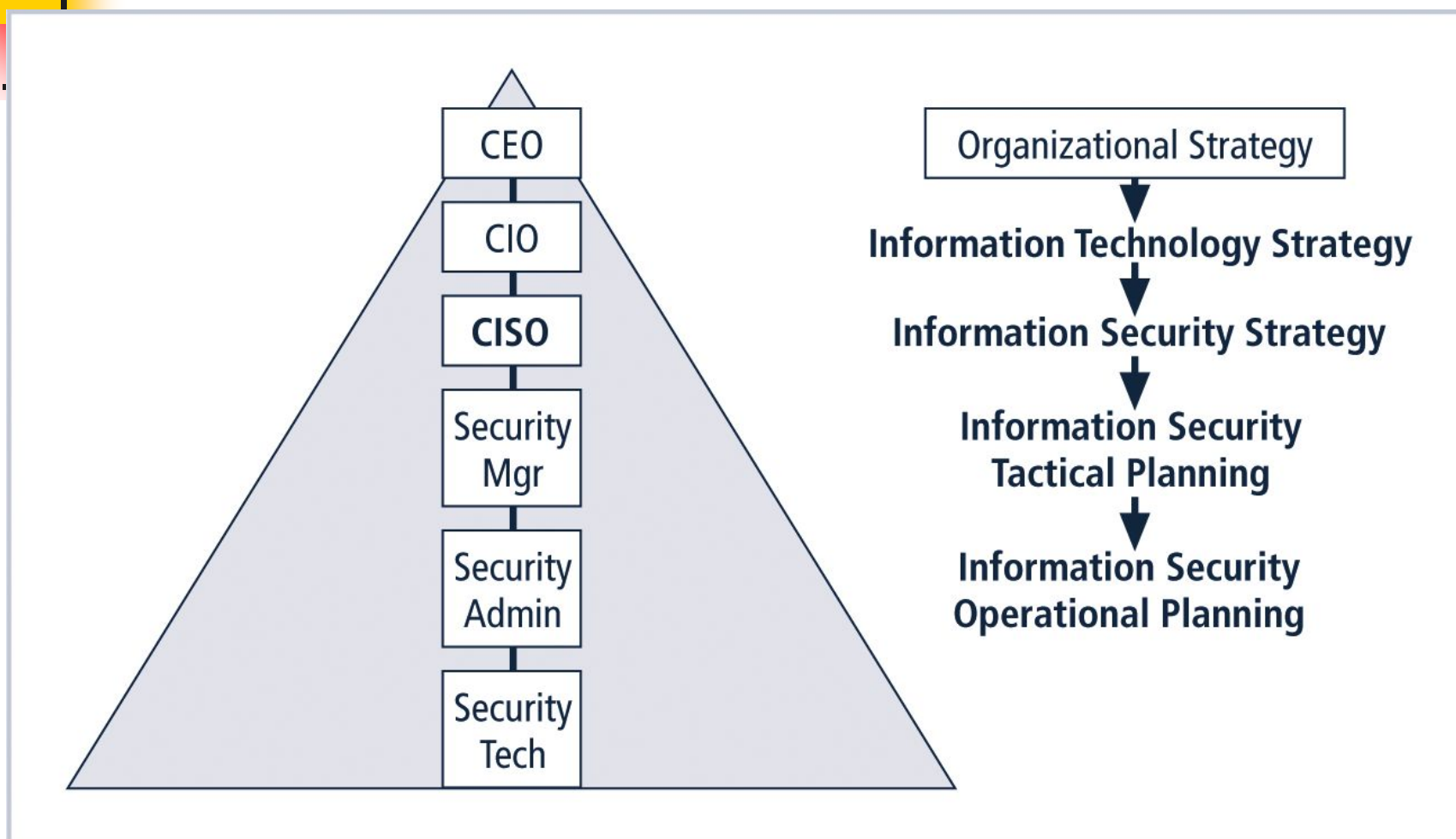


FIGURE 2-3 Top-Down Strategic Planning for Information Security



Strategic Planning

- Organization:
 - Develops a general strategy
 - Creates specific strategic plans for major divisions
- Each level of division
 - translates those objectives into more specific objectives for the level below
- In order to execute this broad strategy,
 - executives must define individual managerial responsibilities

Planning for the Organization

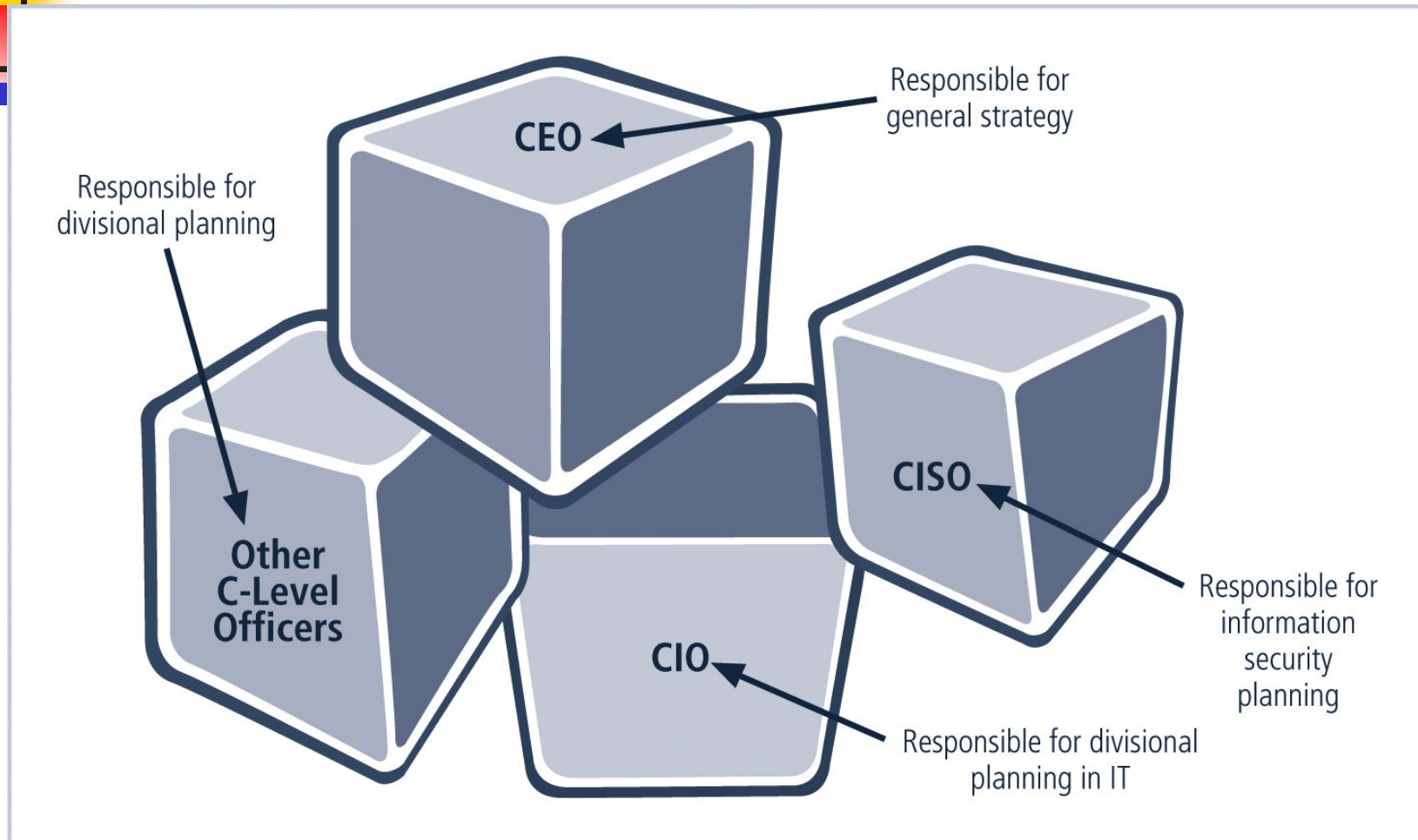


FIGURE 2-4 Planning for the Organization



Strategic Planning

- Strategic goals are translated
 - into tasks with specific, measurable, achievable, reasonably high and time-bound objectives (SMART)
- Strategic planning
 - begins a transformation from general to specific objectives

Planning Levels

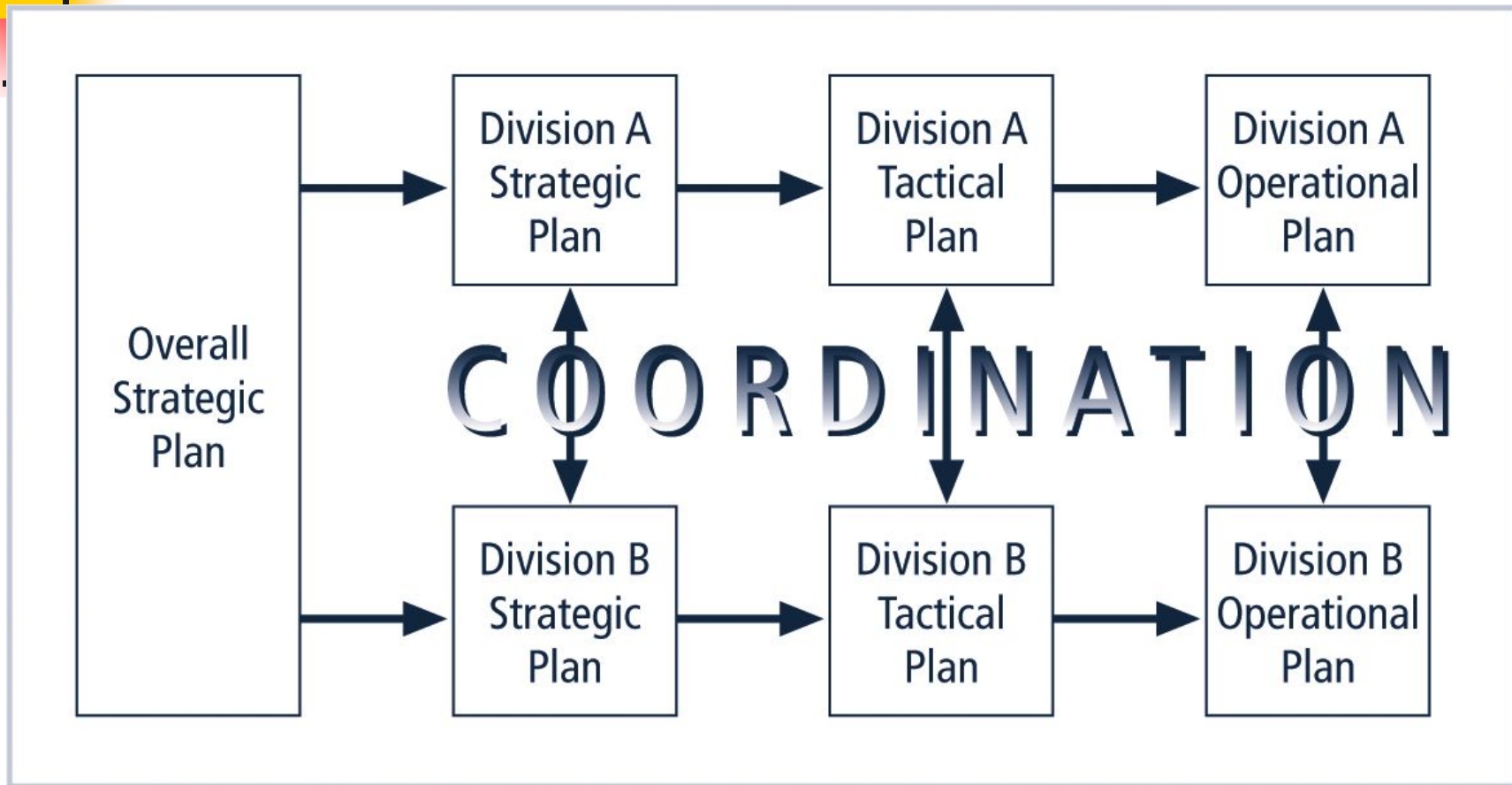


FIGURE 2-5 Planning Levels



Planning levels

- Tactical Planning
 - Shorter focus than strategic planning
 - Usually one to three years
 - Breaks applicable strategic goals into a series of incremental objectives
 - Also called project planning



Planning levels

- Operational Planning
 - Used by managers and employees to organize the ongoing, day-to-day performance of tasks
 - Includes clearly identified coordination activities across department boundaries such as:
 - Communications requirements
 - Weekly meetings
 - Summaries
 - Progress reports



Typical Strategic Plan Elements

Introduction by senior executive (President/CEO)

- Executive Summary
- Mission Statement and Vision Statement
- Organizational Profile and History
- Strategic Issues and Core Values
- Program Goals and Objectives
- Management/Operations Goals and Objectives
- Appendices (optional)
 - Strengths, weaknesses, opportunities and threats (SWOT) analyses, surveys, budgets &etc



Tips For Planning

- Create a compelling vision statement that frames the evolving plan, and acts as a magnet for people who want to make a difference
- Embrace the use of balanced scorecard approach
- Deploy a draft high level plan early, and ask for input from stakeholders in the organization
- Make the evolving plan visible



Tips For Planning

- Make the process invigorating for everyone
- Be persistent
- Make the process continuous
- Provide meaning
- Be yourself
- Lighten up and have some fun



Planning For Information Security Implementation

- The CIO and CISO play important roles
 - in translating overall strategic planning into tactical and operational information security plans
- CISO plays a more active role
 - in the development of the planning details than does the CIO

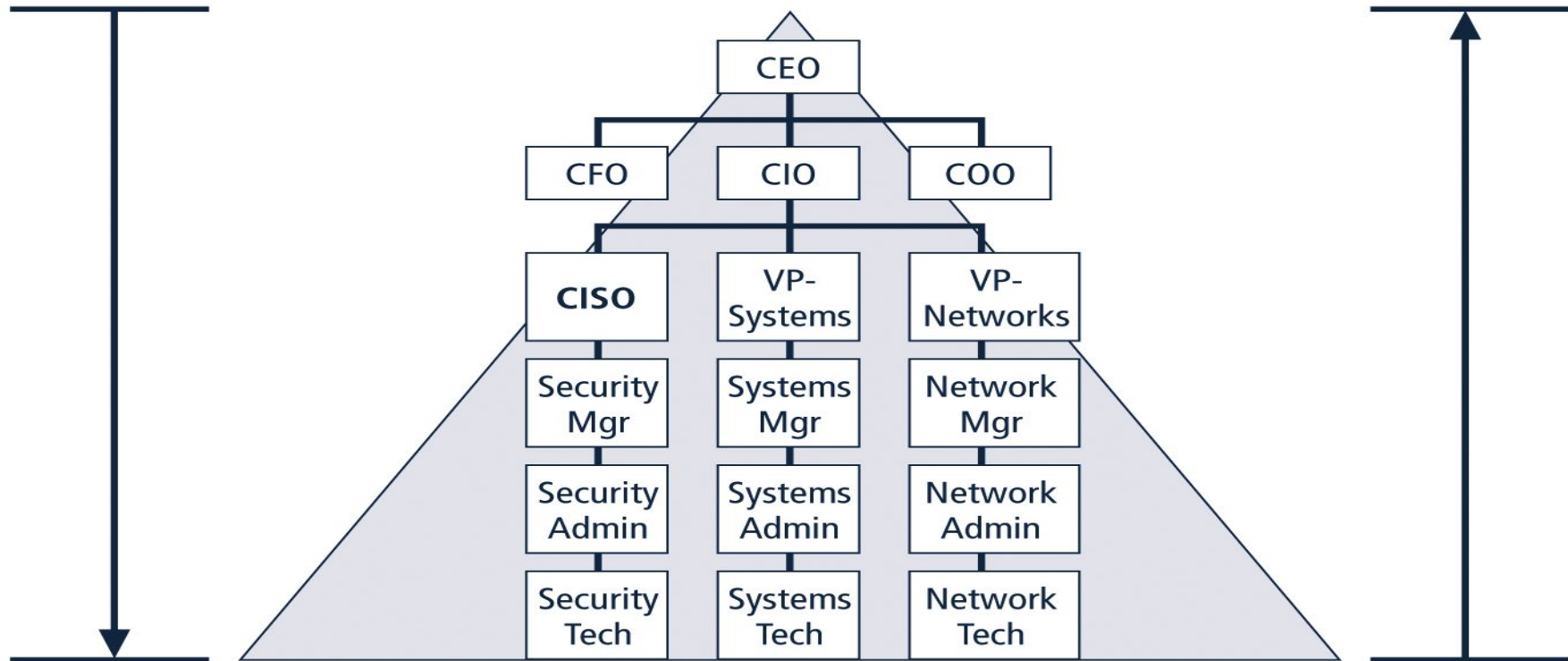


CISO Job Description

- Creates strategic information security plan with a vision for the future of information security at Company X...
- Understands fundamental business activities performed by Company X
 - Based on this understanding, suggests appropriate information security solutions that uniquely protect these activities...
- Develops action plans, schedules, budgets, status reports and other top management communications intended to improve the status of information security at Company X...

Approaches to Security Implementation

Top-down approach –
initiated by top management



Bottom-up approach – initiated by
administrators and technicians

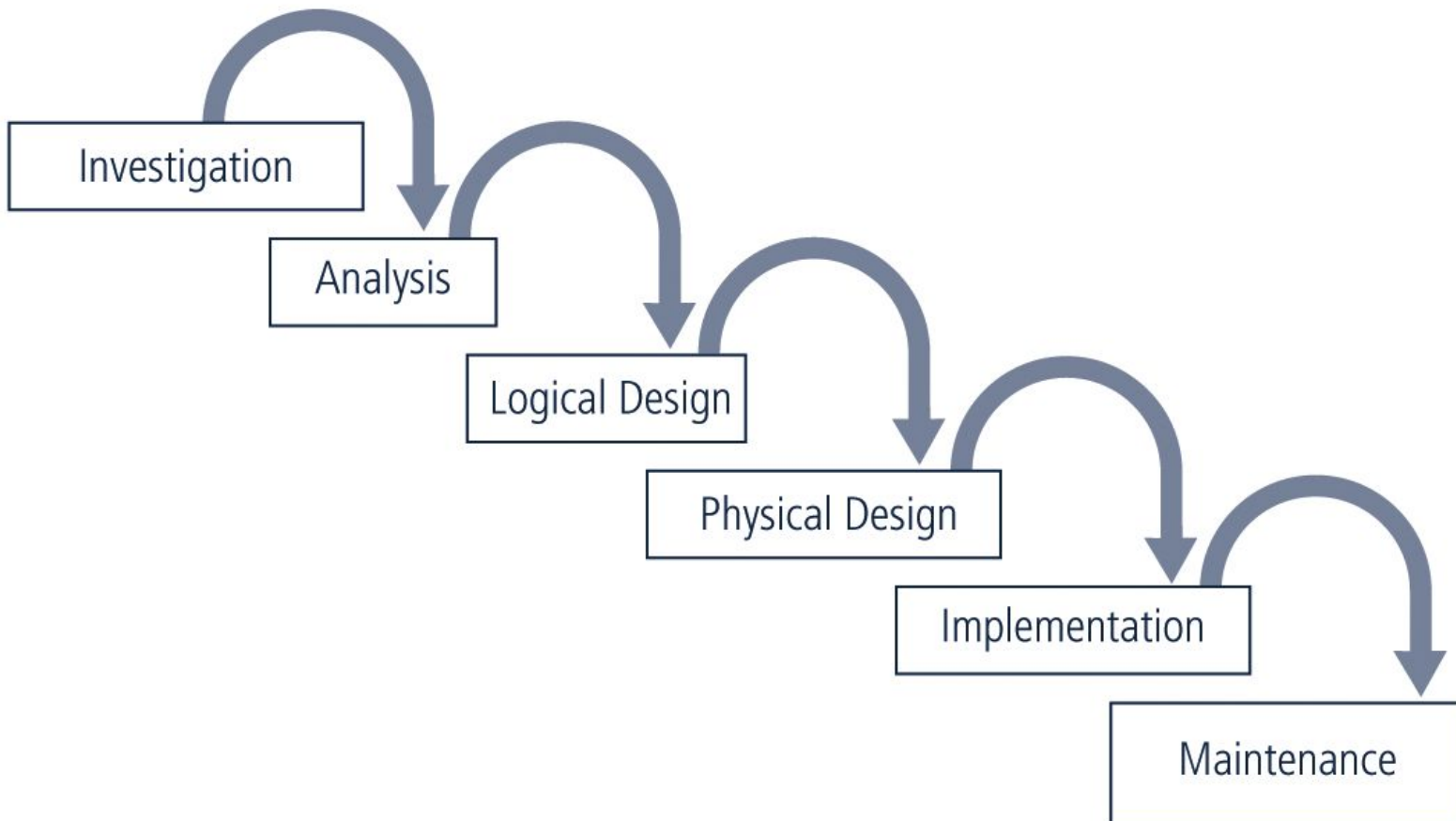
FIGURE 2-7 Approaches to Security Implementation



The Systems Development Life Cycle (SDLC)

- SDLC: methodology for the design and implementation of an information system
- SDLC-based projects may be initiated by events or planned
- Continuous review
 - After each phase
 - determine if the project should be continued, discontinued, outsourced, or postponed

Phases of An SDLC





Investigation

- Identifies problem to be solved
- Begins with the objectives, constraints, and scope of the project
- A preliminary cost/benefit analysis
 - To evaluate the perceived benefits and the appropriate costs for those benefits



Analysis

- Begins with information from the Investigation phase
- Assesses
 - the organization's readiness,
 - its current systems status, and
 - its capability to implement and then support the proposed systems
- Analysts determine
 - what the new system is expected to do, and how it will interact with existing systems



Logical Design

- Information obtained from analysis phase is used to create a proposed solution for the problem
- A system and/or application is selected based on the business need
- The logical design is the *implementation independent* blueprint for the desired solution



Physical Design

- During the physical design phase, the team selects specific technologies
- The selected components are evaluated further as a make-or-buy decision
- A final design is chosen that optimally integrates required components



Implementation

- Develop any software that is not purchased, and create integration capability
- Customized elements are tested and documented
- Users are trained and supporting documentation is created
- Once all components have been tested individually, they are installed and tested as a whole



Maintenance

- Tasks necessary to support and modify the system for the remainder of its useful life
- System is tested periodically for compliance with specifications
- Feasibility of continuance versus discontinuance is evaluated
- Upgrades, updates, and patches are managed
- When current system can no longer support the mission of the organization, it is terminated and a new systems development project is undertaken



The Security Systems DLC

- May differ in several specifics, but overall methodology is similar to the SDLC
- SecSDLC process involves:
 - Identification of specific threats and the risks that they represent
 - Subsequent design and implementation of specific controls to counter those threats and assist in the management of the risk those threats pose to the organization



Investigation in the SecSDLC

- Often begins as directive from management specifying the process, outcomes, and goals of the project and its budget
- Frequently begins with the affirmation or creation of security policies
- Teams assembled to analyze problems, define scope, specify goals and identify constraints
- Feasibility analysis determines whether the organization has resources and commitment to conduct a successful security analysis and design



Analysis in the SecSDLC

- A preliminary analysis of existing security policies or programs is prepared along with known threats and current controls
- Includes an analysis of relevant legal issues that could affect the design of the security solution
- Risk management begins in this stage



Risk Management

- Risk Management: process of identifying, assessing, and evaluating the levels of risk facing the organization
 - Specifically the threats to the information stored and processed by the organization
- To better understand the analysis phase of the SecSDLC, you should know something about the kinds of threats facing organizations
- In this context, a threat is an object, person, or other entity that represents a constant danger to an asset



Key Terms

- **Attack**: deliberate act that exploits a vulnerability to achieve the compromise of a controlled system
 - Accomplished by a **threat agent** that damages or steals an organization's information or physical asset
- **Exploit**: technique or mechanism used to compromise a system
- **Vulnerability**: identified weakness of a controlled system in which necessary controls are not present or are no longer effective

Threats to Information Security

TABLE 2-1 Threats to Information Security¹²

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Deviations in quality of service from service providers	Power and WAN service issues
9. Forces of nature	Fire, flood, earthquake, lightning
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies



Some Common Attacks

- Malicious code
- Hoaxes
- Back doors
- Password crack/Brute force/Dictionary
- Denial-of-service (DoS) and distributed denial-of-service (DDoS)
- Spoofing
- Man-in-the-middle
- Spam
- Mail bombing
- Sniffer
- Social engineering
- Buffer overflow
- Timing



Risk Management

- Use some method of prioritizing risk posed by each category of threat and its related methods of attack
- To manage risk, you must **identify** and **assess** the value of your information assets
- Risk assessment assigns comparative risk rating or score to each specific information asset



Design in the SecSDLC

- Design phase consists of two distinct phases:
 - **Logical design phase:** team members create and develop a blueprint for security, and examine and implement key policies
 - **Physical design phase:** team members evaluate the technology needed to support the security blueprint, generate alternative solutions, and agree upon a final design



Security Models

- Security managers often use established security models to guide the design process
- Security models provide frameworks for ensuring that all areas of security are addressed
- Organizations can adapt or adopt a framework to meet their own information security needs



Policy

- A critical design element of the information security program is the information security policy
- Management must define three types of security policy:
 - General or security program policy
 - Issue-specific security policies
 - Systems-specific security policies



SETA

- An integral part of the InfoSec program is
 - Security education and training (SETA) program
 - SETA program consists of three elements:
 - security education, security training, and security awareness
- Purpose of SETA is to enhance security by:
 - Improving awareness
 - Developing skills and knowledge
 - Building in-depth knowledge



Design

- Design
 - Focuses on controls and safeguards used to protect information from attacks by threats
- Three categories of controls:
 - Managerial
 - Operational
 - Technical



Managerial Controls

- Address design/implementation of the
 - security planning process and
 - security program management
- Risk management
- Security control reviews
- Legal compliance and maintenance of the entire security life cycle



Operational Controls

- Cover management functions and lower level planning including:
 - Disaster recovery
 - Incident response planning
 - Personnel security
 - Physical security
 - Protection of production inputs and outputs
 - Provide structure for the development of SETA
 - Hardware/software maintenance and data integrity



Technical Controls

- Address those tactical and technical issues related to
 - designing and implementing security in the organization
- Technologies necessary to protect information are examined and selected



Contingency Planning

- Essential preparedness documents provide contingency planning (CP) to prepare, react and recover from circumstances that threaten the organization:
 - Incident response planning (IRP)
 - Disaster recovery planning (DRP)
 - Business continuity planning (BCP)



Physical Security

- Physical Security addresses
 - the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization
- Physical resources include:
 - People
 - Hardware
 - Supporting information system elements



Implementation in the SecSDLC

- Security solutions are acquired, tested, implemented, and tested again
- Personnel issues are evaluated and specific training and education programs conducted
- Perhaps most important element of implementation phase is management of project plan:
 - Planning the project
 - Supervising tasks and action steps within the project
 - Wrapping up the project



InfoSec Project Team

- Should consist of individuals experienced in one or multiple technical and non-technical areas including:
 - Champion
 - Team leader
 - Security policy developers
 - Risk assessment specialists
 - Security professionals
 - Systems administrators
 - End users



Staffing the InfoSec Function

- Each organization should examine the options for staffing of the information security function
 1. Decide how to position and name the security function
 2. Plan for proper staffing of information security function
 3. Understand impact of information security across every role in IT
 4. Integrate solid information security concepts into personnel management practices of the organization



InfoSec Professionals

- It takes a wide range of professionals to support a diverse information security program:
 - Chief Information Officer (CIO)
 - Chief Information Security Officer (CISO)
 - Security Managers
 - Security Technicians
 - Data Owners
 - Data Custodians
 - Data Users



Certifications

- Many organizations seek professional certification so that they can more easily identify the proficiency of job applicants:
 - CISSP
 - SSCP
 - GIAC
 - SCP
 - ICSA
 - Security +
 - CISM



Maintenance and Change in the SecSDLC

- Once information security program is implemented,
 - it must be properly operated, managed, and kept up to date by means of established procedures
- If the program is not adjusting adequately to the changes in the internal or external environment, it may be necessary to begin the cycle again



Maintenance Model

- While a systems management model is designed to manage and operate systems, a maintenance model is intended to focus organizational effort on system maintenance:
 - External monitoring
 - Internal monitoring
 - Planning and risk assessment
 - Vulnerability assessment and remediation
 - Readiness and review
 - Vulnerability assessment

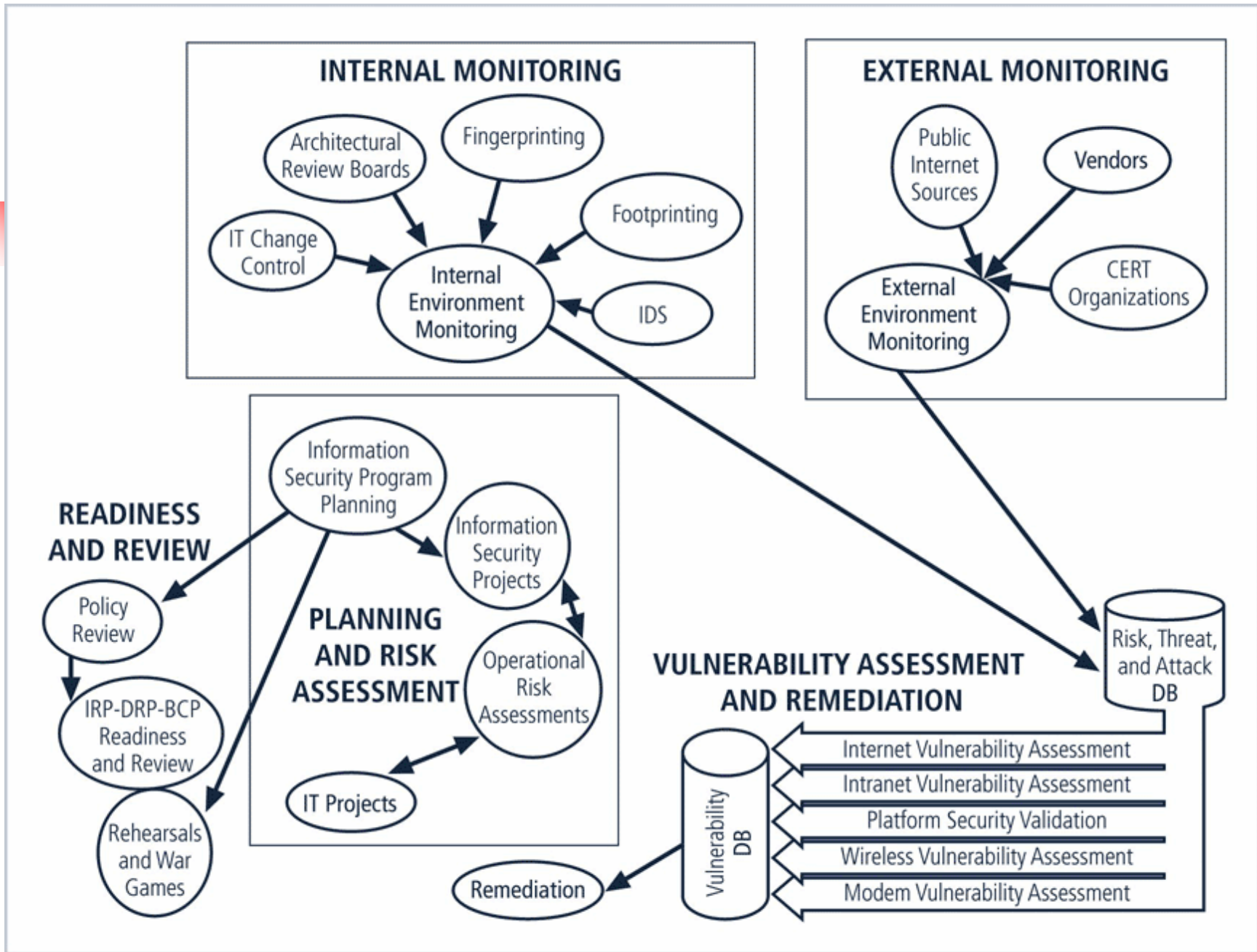


FIGURE 2-10 Maintenance Model



ISO Management Model

- One issue planned in the SecSDLC is the systems management model
- ISO network management model - five areas:
 - Fault management
 - Configuration and name management
 - Accounting management
 - Performance management
 - Security management



Security Management Model

- **Fault Management** involves identifying and addressing faults
- **Configuration and Change Management** involve administration of components involved in the security program and administration of changes
- **Accounting and Auditing Management** involves chargeback accounting and systems monitoring
- **Performance Management** determines if security systems are effectively doing the job for which they were implemented



Security Program Management

- Once an information security program is functional, it must be operated and managed
 - a formal management standard can provide some insight into the processes and procedures needed
 - Some options:
 - Based on the BS7799/ISO17799 model or the NIST models described earlier
- Handout
 - Comparison between SDLC and SecSDLC