# Protection

- Risk management activities, including
  - risk assessment and controls, and
- **Protection** mechanisms, technologies & tools
  - Each of these mechanisms represents some aspect of the management of specific controls in the overall security plan

# People

- **People** are the most critical link in the information security program
- It is imperative that managers continuously recognize the crucial role that people play; includes
  - information security personnel and the security of personnel, as well as aspects of the SETA program

# Project Management

- **Project management** discipline should be present throughout all elements of the information security program

- Involves
  - Identifying and controlling the resources applied to the project
  - Measuring progress and adjusting the process as progress is made toward the goal

# 2. Security Planning

# Outline

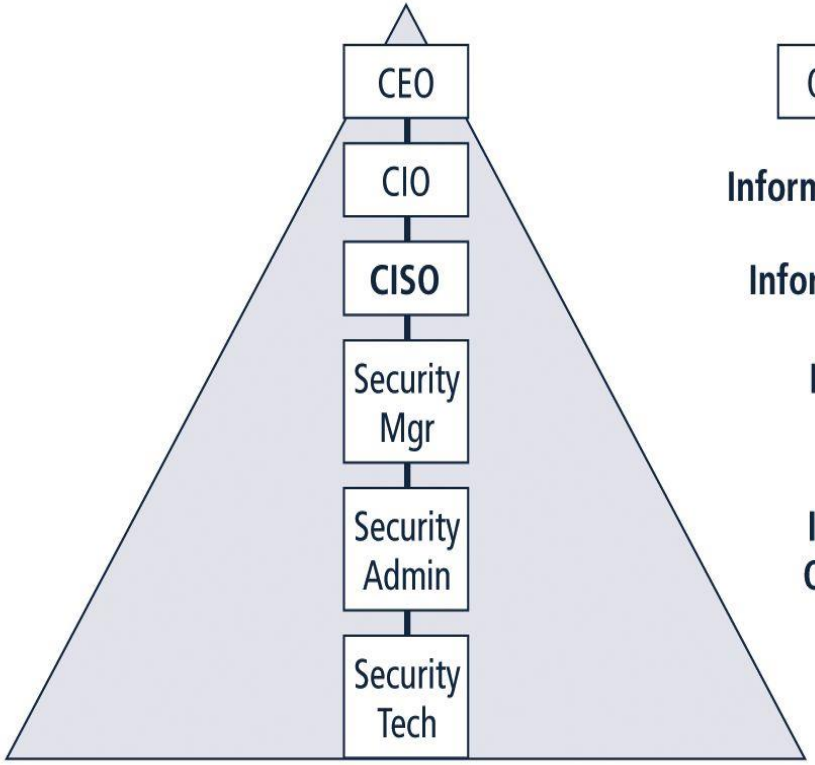
1. Introduction
2. Organizational Planning
3. The Security SDLC

# 1. Introduction

- **Planning:**
  - Is creating action steps toward goals, and then controlling them

- Planning process
  1. Organizational planning (in general and specific to information security)
  2. Preparedness planning, also called **contingency planning**.

# 2. Organizational Planning





1. Strategic
2. Tactical
3. Operational

# Strategic Planning

- Strategy is the basis for long-term direction

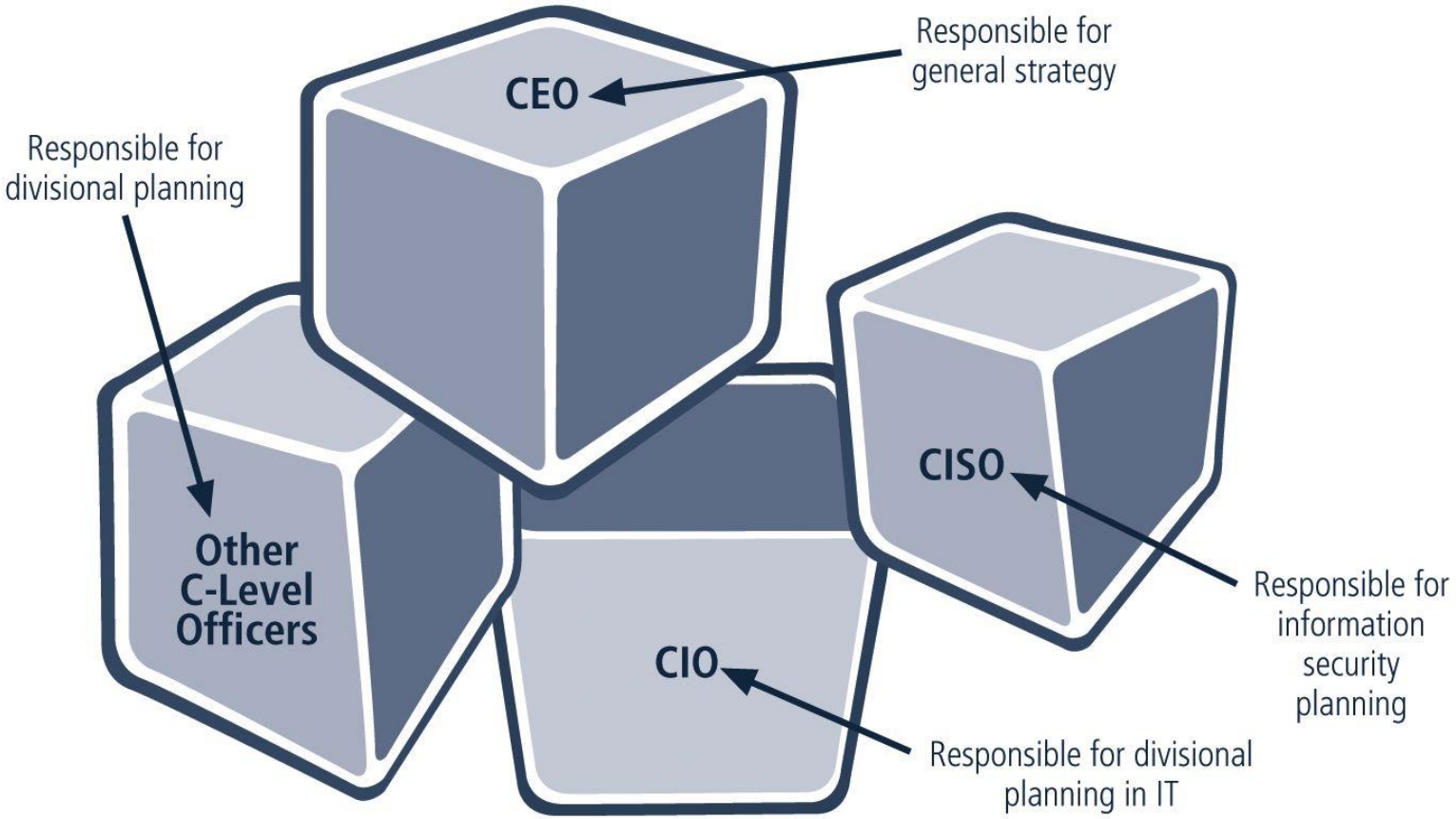
- Strategic planning:
  - Guides organizational efforts
  - Focuses resources on clearly defined goals

  "… 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

- 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

# Strategic Planning



# Tactical Planning

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

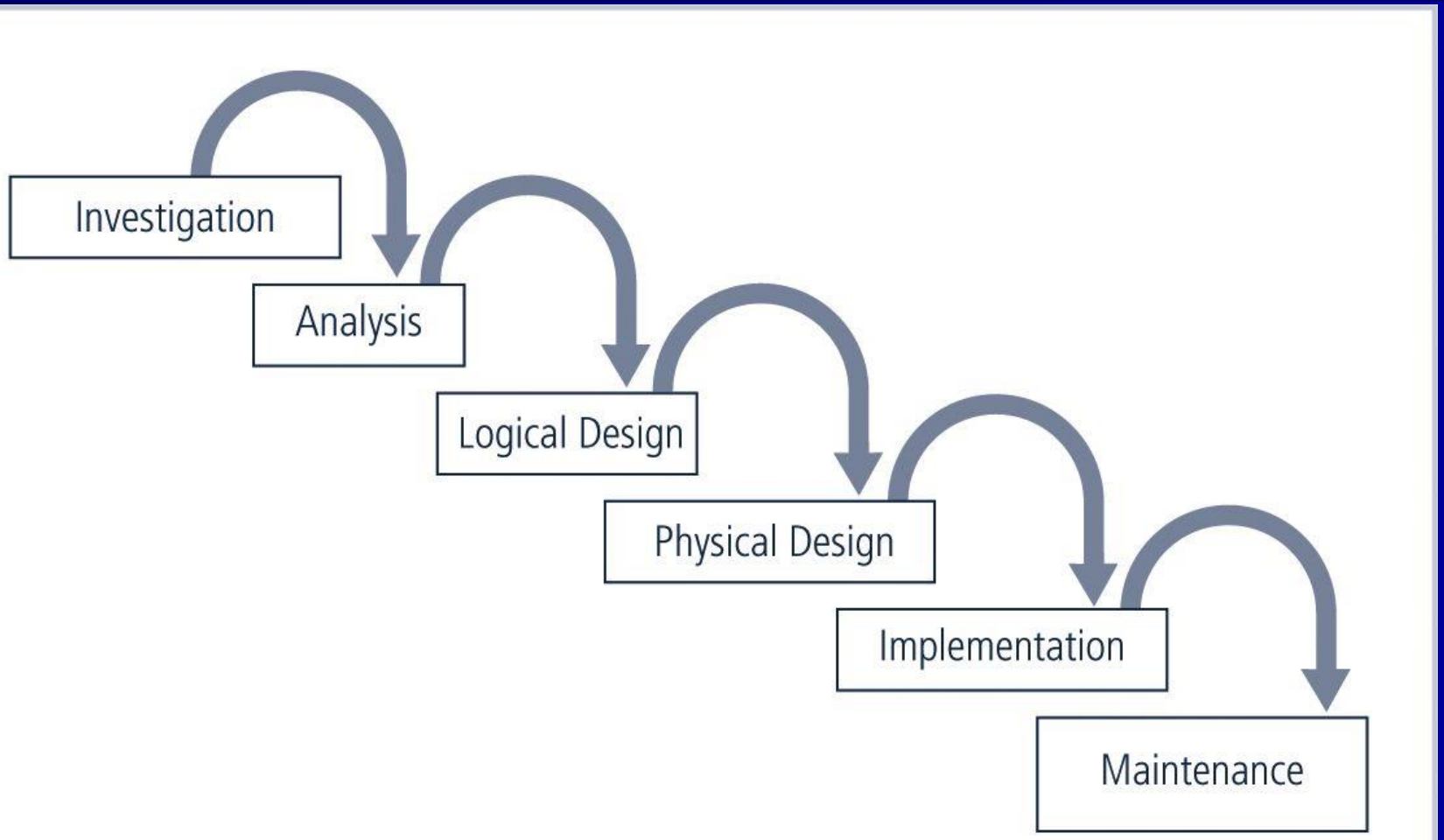
# Operational Planning

- 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

# 3. The Security SDLC

- In general, the Security SDLC is similar to the SDCL
  - A methodology for the design and implementation of an information system in an organization.
- 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

# SecSDLC


Investigation
Analysis
Logical Design
Physical Design
Implementation
Maintenance

# Investigation in the SecSDLC

- **Investigation** 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

# 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

  Risk management identifies vulnerabilities in an organization's information systems and takes carefully reasoned steps to assure the confidentiality, integrity, and availability of all the components in organization's information system

# Design in the SecSDLC

- Design phase actually 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

- Between the logical and physical design phases, a security manager may seek to use established **security models** to guide the design process.

# 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