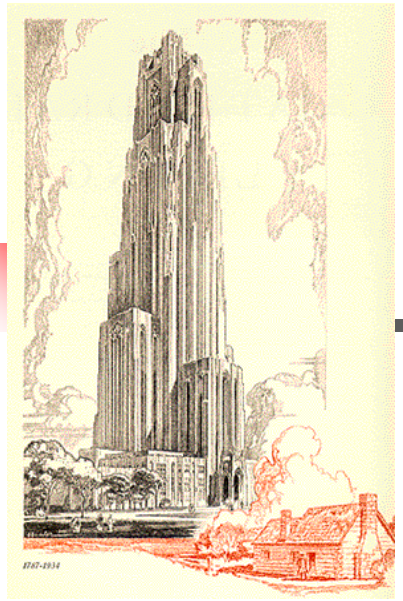
TEL2813/IS2621
Security Management

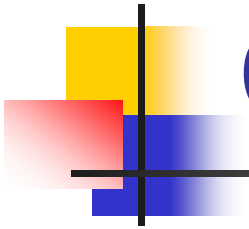


James Joshi
Associate Professor

Lecture 1

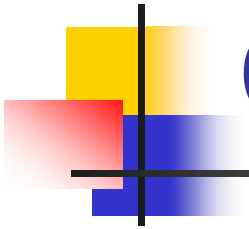
Jan 8, 2015

Introduction to
Security Management & Security Planning



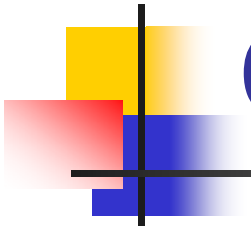
Contact

- James Joshi
  - 706A, IS Building
  - Phone: 412-624-9982
  - E-mail: jjoshi@mail.sis.pitt.edu
- Course Web: http://www.sis.pitt.edu/~jjoshi/courses/IS2621/Spring2014/
- Office Hours:
  - By appointments OR just drop by
- GSA help:
  - Lei Jin



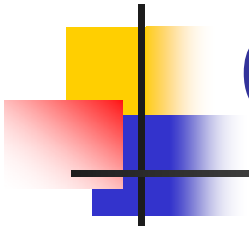
Course objective

- The course is aimed at imparting knowledge and skill sets
  - required to assume the overall responsibilities of security administration and management of security of an enterprise information system.
  - Related to
    - Computer forensics
    - Legal, policy, compliance and certification issues



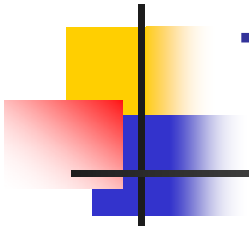
Course objective

- Carry out a detailed analysis of cyber defense operations and planning, and enterprise security management by performing various types of analysis such as vulnerability analysis, penetration testing, audit trail analysis, system and network monitoring, and configuration management.
- Carry out detailed risk analysis and assessment of enterprise systems using various practical and theoretical tools.
- Understand and employ tools for forensics, including host forensics, network forensics, device and media forensics
- Understanding of how to make enterprise wide security plans and policies, and deploy appropriate safeguards (models, mechanisms and tools) at all the levels by providing due consideration to the life-cycle of the enterprise information systems and networks, as well as its legal and social environment.



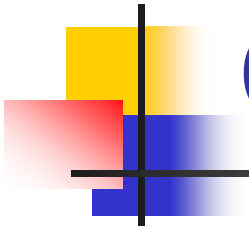
Course Objective/Material

- See course webpage for the
  - list of topics and
  - Initial list of references on webpage
- A lot of reading materials (journal, articles, etc., will be expected)
- Some topic may be covered as presentation/reading assignments
- Several labs assignments



Tentative Grading

- Assignments (50%)
  - Homework/Quiz/Paper review/Lab (35%)
  - Class Participation/Seminar attendance (5%)
  - About 2 presentations (10%)
- Exams 20%
- Project 30%



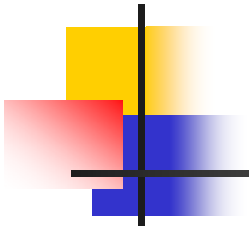
Course Policies

- Your work MUST be your own
  - Zero tolerance for cheating/plagiarism
  - You get an F for the course if you cheat in anything however small – NO DISCUSSION
  - Discussing the problem is encouraged
- Homework
  - Penalty for late assignments (15% each day)
  - Ensure clarity in your answers – no credit will be given for vague answers
  - Homework is primarily the GSA's responsibility
- Check webpage for everything!
  - You are responsible for checking the webpage for updates

Introduction to Security Management

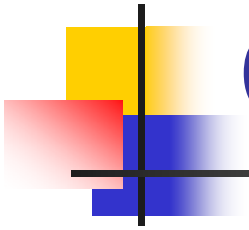
Acknowledgement:

From Book “Management of Information Security” by Whitman



Introduction

- Information security involves three distinct communities of interest
  - Information security managers and professionals
  - Information technology managers and professionals
  - Non-technical business managers and professionals



Communities of Interest

- InfoSec community:
  - protect information assets from threats
- IT community:
  - support business objectives by supplying appropriate information technology
- Business community:
  - policy and resources

Security and Control

- Examples
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
- Controls
  - Physical
  - Technical
  - Administrative/procedural
  - Prevention – Detection – Recovery
  - Deterrence, Corrective

InfoSec Components

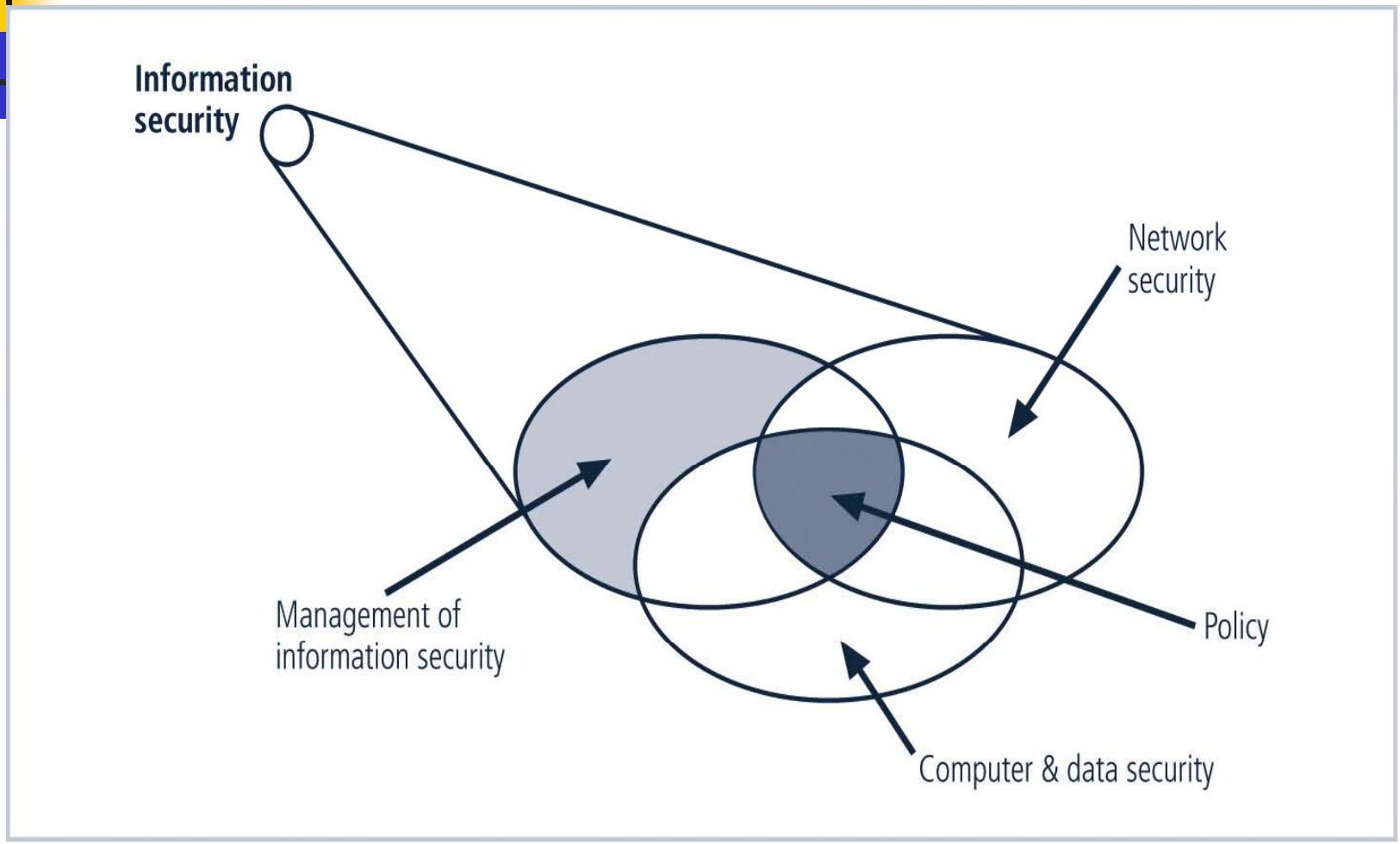
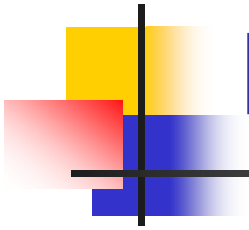


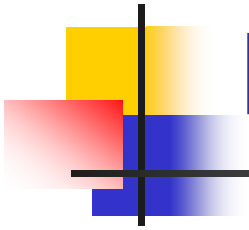
FIGURE 1-1 Components of Information Security



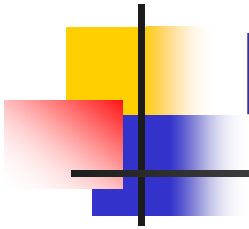
Key Concepts: Confidentiality

- Confidentiality
  - only those with sufficient privileges may access certain information
- Confidentiality model
  - Bell-LaPadula
    - No write down & No read up
  - TCSEC/TNI (Orange, Red Book)
- Some threats
  - Hackers
  - Masqueraders
  - Unauthorized users
  - Unprotected download of files
  - LANS
  - Trojan horses

Key Concepts: Integrity



- Integrity
  - Integrity is the quality or state of being whole, complete, and uncorrupted
- Integrity model
  - Biba/low water mark
    - No write up & No read down
  - Clark-Wilson
    - Separation of duty
  - Lipner
- Other issues
  - Origin integrity
  - Data integrity



Key Concepts

- Confidentiality
- Integrity
- Availability
- Survivability
- Accountability
- Privacy
- Authentication
- Authorization
- Accountability
- Assurance

What Is Management?

- A process of achieving objectives using a given set of resources
- A manager is
  - “someone who works with and through other people by coordinating their work activities in order to accomplish organizational goals”

Managerial Roles

- Informational role:
  - Collecting, processing, and using information to achieve the objective
- Interpersonal role:
  - Interacting with superiors, subordinates, outside stakeholders, and others
- Decisional role:
  - Selecting from alternative approaches and resolving conflicts, dilemmas, or challenges

Differences Between Leadership and Management

- Leadership
  - provides purpose, direction, and motivation to those that follow
- The leader
  - influences employees towards achieving objectives
  - expected to lead by example and demonstrate personal traits that makes others to follow
- A manager
  - administers the resources of the organization, budgets, authorizes expenditure

Characteristics of a Leader

1. Bearing
2. Courage
3. Decisiveness
4. Dependability
5. Endurance
6. Enthusiasm
7. Initiative
8. Integrity
9. Judgment
10. Justice
11. Knowledge
12. Loyalty
13. Tact
14. Unselfishness

Used by US military

Leadership quality and types

- A leader must:
  - BE a person of strong and honorable character
  - KNOW the details of your situation, the standards to which you work, human nature, and your team
  - DO by providing purpose, direction, and motivation to your team
- Three basic behavioral types of leaders:
  - Autocratic
  - Democratic
  - Laissez-faire

Characteristics of Management

- Two management approaches :
  - Traditional management theory using principles of
    - planning, organizing, staffing, directing, and controlling (POSDC)
  - Popular management theory using principles of
    - management into planning, organizing, leading, and controlling (POLC)

The Planning–Controlling Link

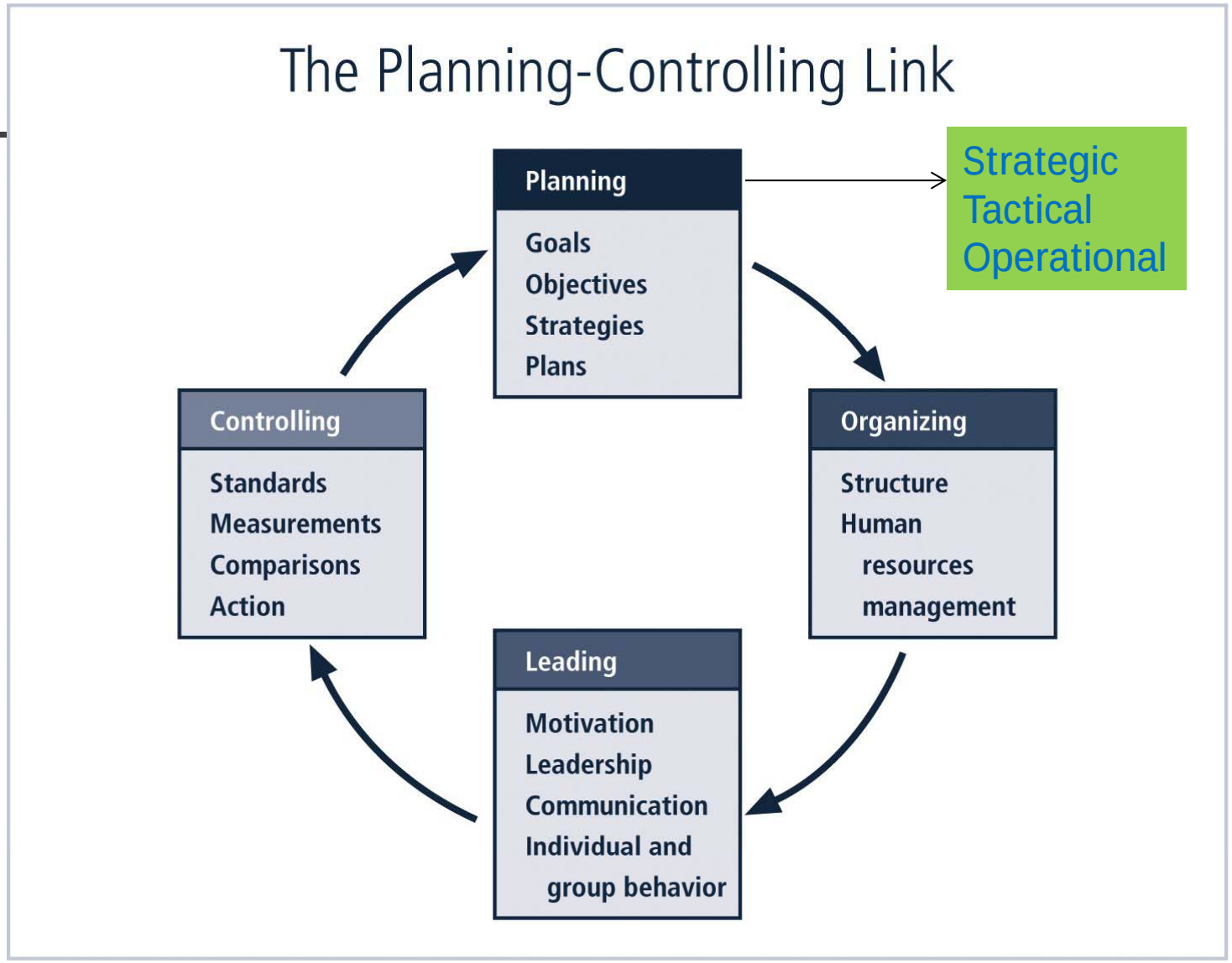
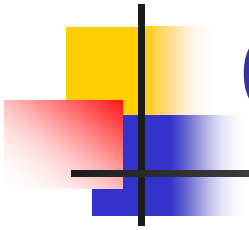


FIGURE 1-3 The Planning-Controlling Link[8]



Control Tools

- Four categories:
  - Information
    - Information flows/ communications
  - Financial
    - Guide use of monetary resources (ROI,CBA,..)
  - Operational
    - PERT, Gantt, process flow
  - Behavioral
    - Human resources

The Control Process

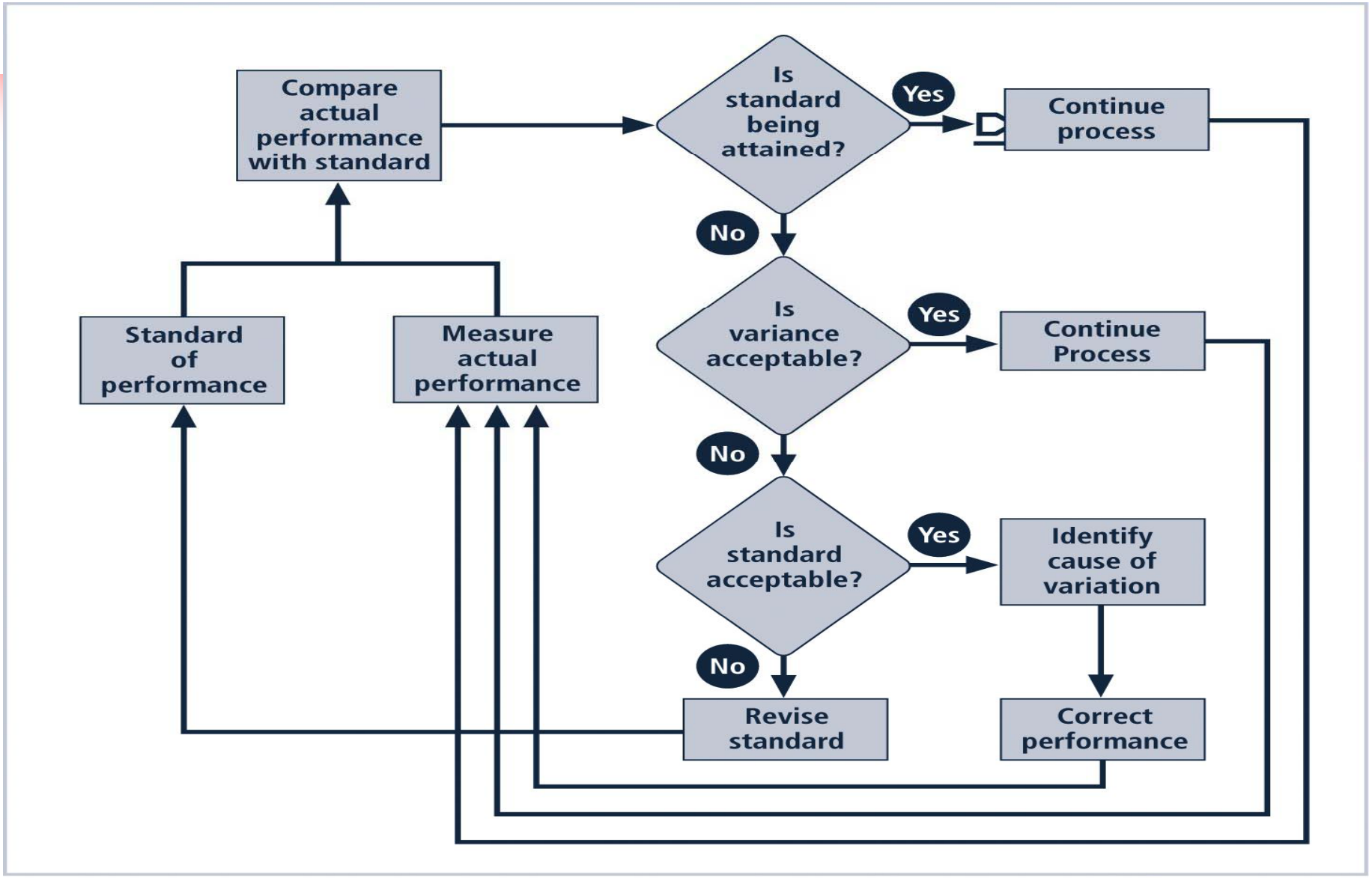
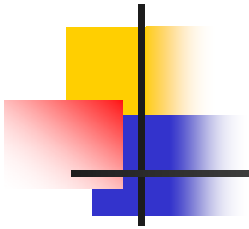


FIGURE 1-4 The Control Process

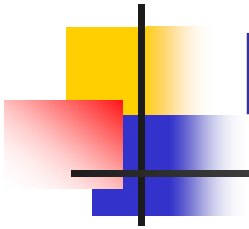
Principles Of Information Security Management

- The extended characteristics of information security are known as the six Ps:
  - Planning
  - Policy
  - Programs
  - Protection
  - People
  - Project Management



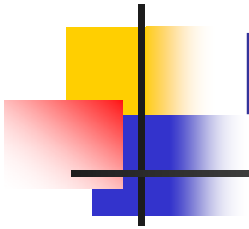
InfoSec Planning

- Several types of InfoSec plans exist:
  - Incident response
  - Business continuity
  - Disaster recovery
  - Policy
  - Personnel
  - Technology rollout
  - Risk management and
  - Security program including education, training and awareness



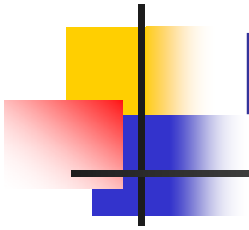
Policy

- Policy
  - set of organizational guidelines that dictates certain behavior within the organization
- Three general categories of policy:
  - General policy (Enterprise Security Policy)
  - An issue-specific security policy (ISSP)
    - E.g., email, Internet use
  - System-specific policies (SSSPs)
    - E.g., Access control list (ACLs) for a device



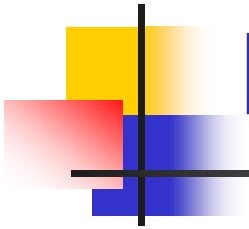
Programs

- Programs are operations managed as
  - Specific entities in the information security domain
  - Example:
    - A security education training and awareness (SETA) program is one such entity
  - Other programs that may emerge include
    - a physical security program, complete with fire, physical access, gates, guards, and so on



Protection

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

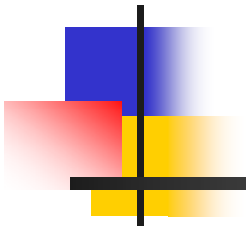


People

- People are the most critical link in the information security program
  - Human firewall
- 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
  - 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 it as needed towards achieving the goal



Security Planning

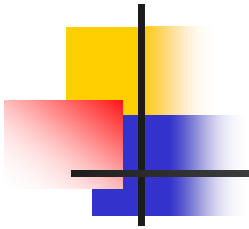
Introduction

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

Supply Chain Security is a growing concern

Introduction

- Planning involves:
  - 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

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
    - (Pitt CSSD) Providing innovative information technology services to support learning, teaching, research, and business at the University of Pittsburgh.

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 & C-Level functions

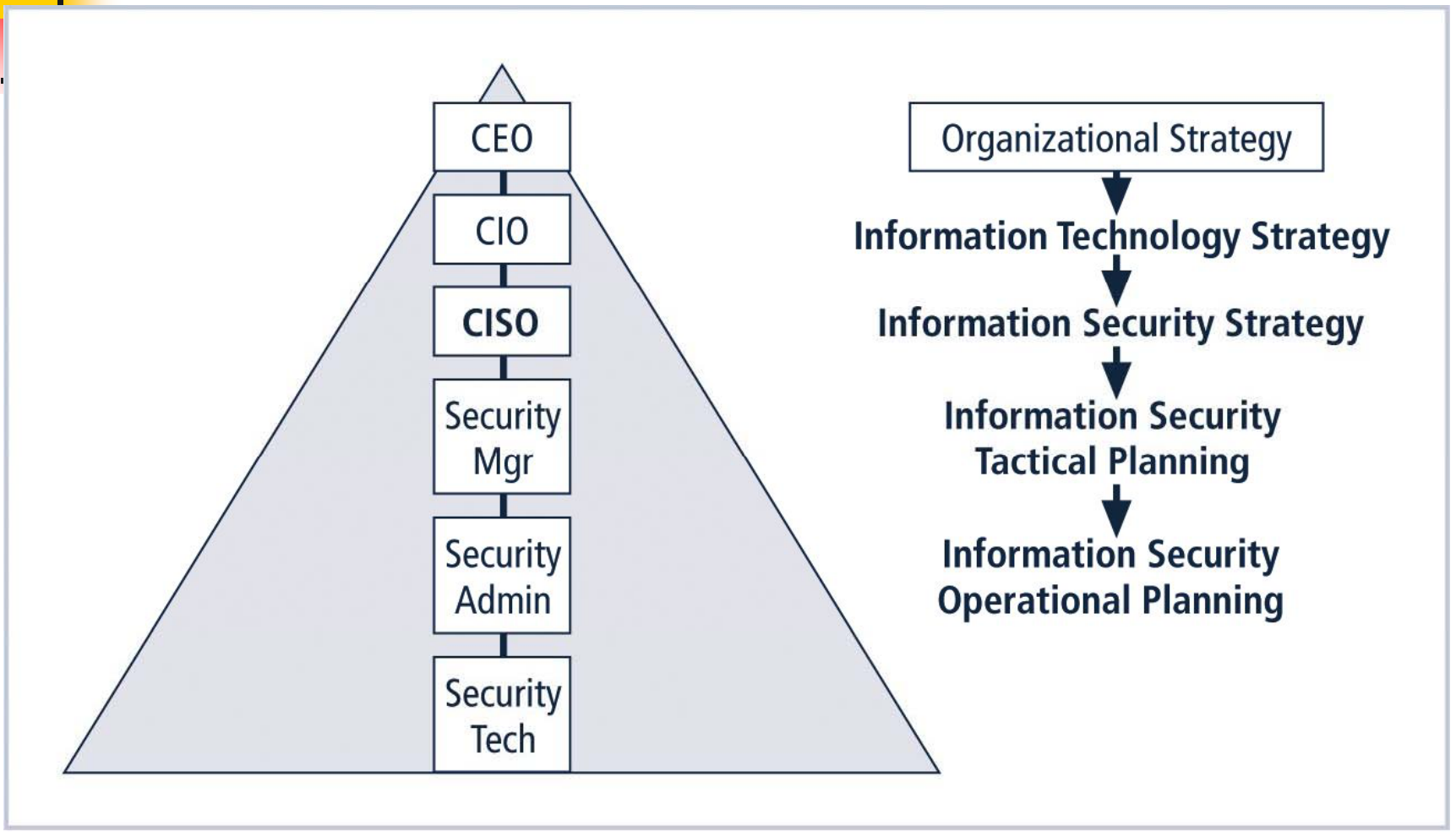


FIGURE 2-3 Top-Down Strategic Planning for Information Security

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
- Execution of broad strategy
  - executives must define individual managerial responsibilities

Example

- Providing the highest quality healthcare service in the industry ← CEO
- Providing high-level health care service in support of the highest quality healthcare service in the industry ← CIO
- Providing the highest –quality medical service ← COO
- Ensuring that health care information services are provided securely and in conformance with all state and federal information processing, information security, and privacy statues, specifically including HIPPA Compliance ← CISO

Strategic Planning

- Strategic goals are translated into
  - Specific, Measurable, Achievable, Reasonably high and Time-bound objectives (SMART)
- Strategic planning
  - begins a transformation from general to specific objectives

Planning Levels

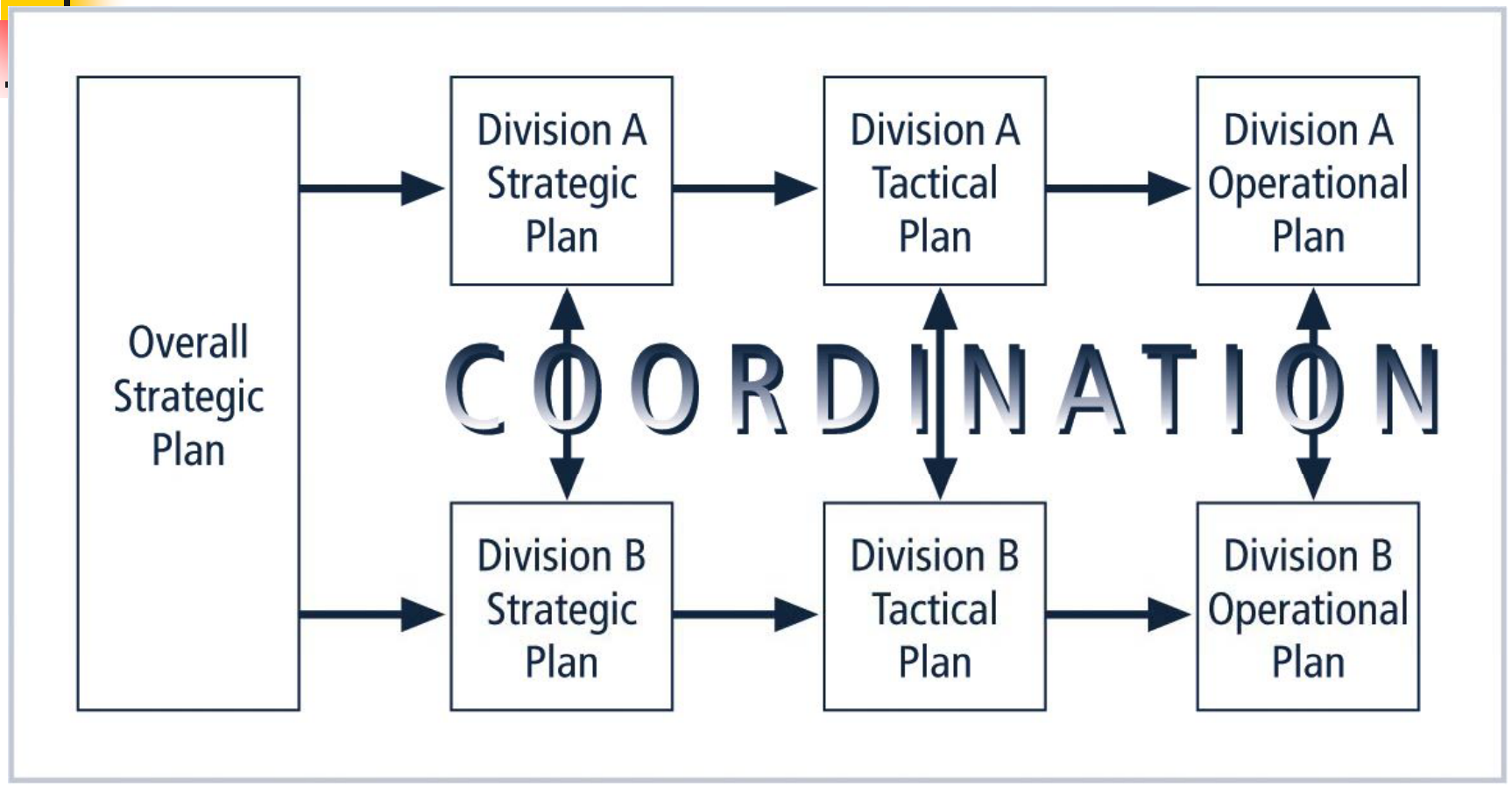
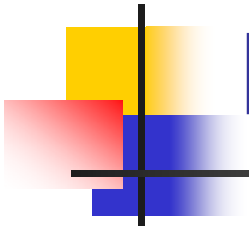


FIGURE 2-5 Planning Levels



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
  - 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

- CIO and CISO play important roles
  - Translate 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

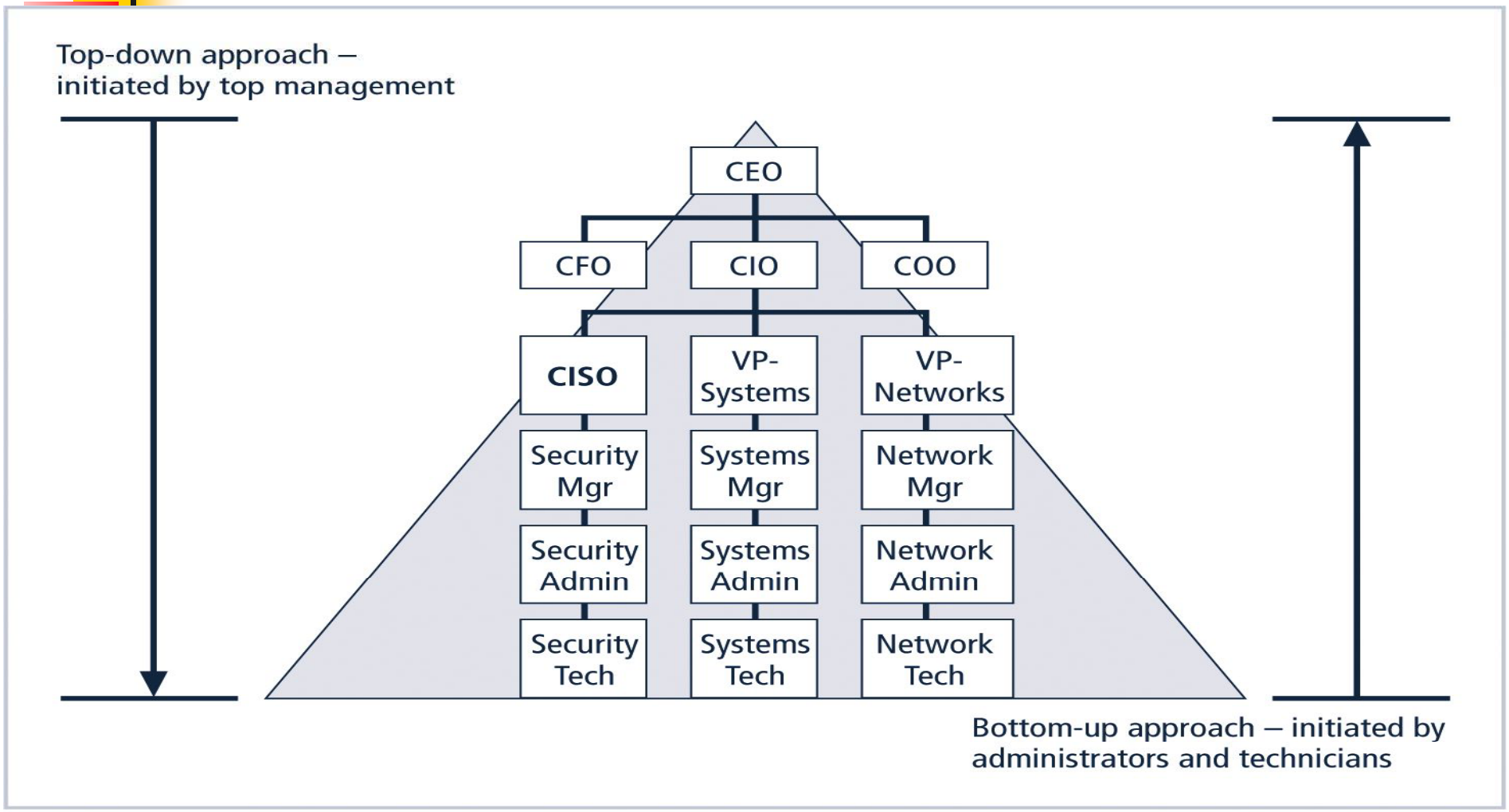
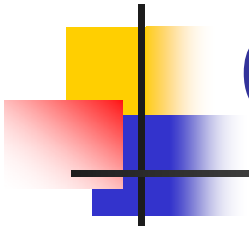


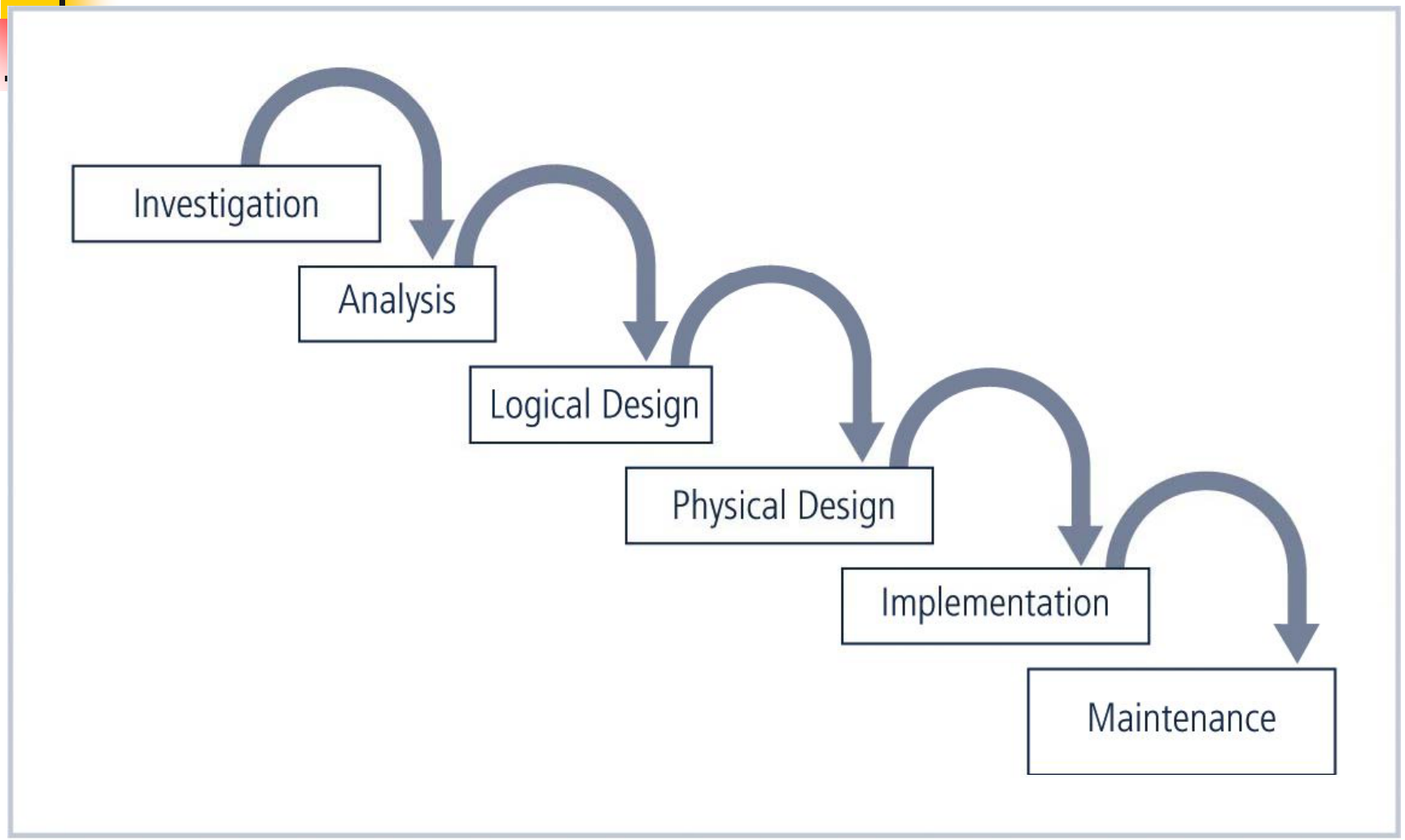
FIGURE 2-7 Approaches to Security Implementation

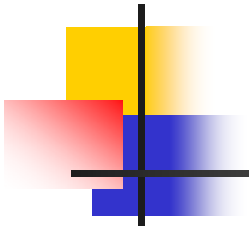
The Systems Development Life Cycle (SDLC)



- 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

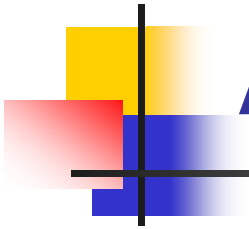
Phases of An SDLC





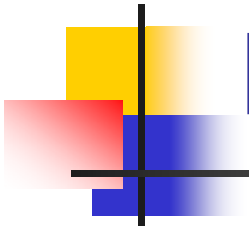
Investigation

- 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



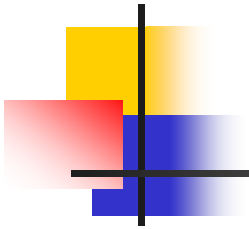
Analysis

- 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
- Determine
  - what the new system is expected to do, and how it will interact with existing systems



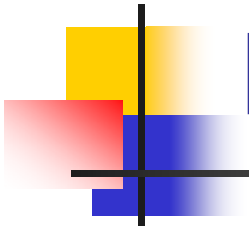
Logical/Physical Design

- Logical design is the *implementation independent* blueprint for the desired solution
  - Use Information obtained from analysis phase
- Physical Design
  - Select specific technologies
  - Evaluated further as a make-or-buy decision
  - Final design should optimally integrates required components



Implementation

- Key steps
  - Develop any software that is not purchased, and create integration capability
  - Test and document customized elements
  - Train users and create supporting documentation
  - Installed and tested as a whole



Maintenance

- Tasks necessary to support and modify the system for the remainder of its useful life
- Test periodically for compliance with specification
- Evaluate feasibility of continuance versus discontinuance
- Manage upgrades, updates, and patches
- If current system can no longer support the mission:
  - Undertake 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
  - Design and implementation of specific controls to mitigate identified 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
  - Also specify the process, outcomes, and goals of the project and its budget
- May also begin 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

- Conduct preliminary analysis
  - of existing security policies or programs
  - identify known threats and current controls
  - Analyze relevant legal issues that could affect the design of the security solution
- Initiate risk management
  - Assessment, Mitigation Strategies, etc.

Risk Management

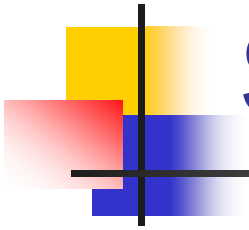
- Risk Management:
  - process of identifying, assessing, and evaluating the levels of risk facing the organization
  - A threat is an object, person, or other entity that represents a constant danger to an asset

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

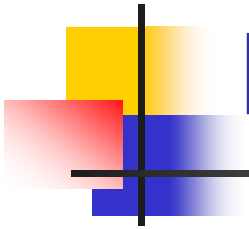
Design in the SecSDLC

- 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



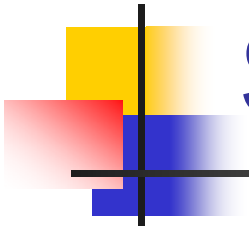
Security Models

- 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



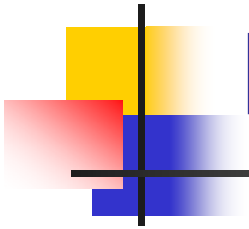
Policy

- 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

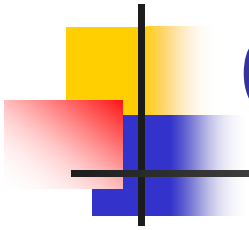
  - Legal compliance and maintenance of the entire security life cycle

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

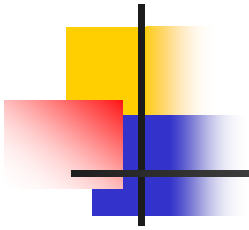
- Essential preparedness documents provide contingency planning (CP) to prepare, react and recover from circumstances that threaten the organization:
  - Incident response planning (IRP)
  - Disaster recovery planning (DRP)
  - Business continuity planning (BCP)

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 this phase is management of project plan:
  - Planning the project
  - Supervising tasks and action steps within
  - Wrapping up the project



InfoSec Project Team

- Should consist of individuals experienced in one or multiple technical and non-technical areas; include:
  - 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

National Cybersecurity Workforce Framework
http://csrc.nist.gov/nice/framework/

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

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 (Certified Info Sys Sec Professional)
  - SSCP (Sys Sec Certified Practioner)
  - GIAC (Global Info Assurance Certification)
  - SCP (Security Certified Professional)
  - ICSA (International Computer Security Ass.)
  - Security +
  - CISM (Certified Info Sec Manager)
  - CISA (Certified Info Systems Auditor)

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
- Continuous improvement/evolution
  - If the program is not adjusting adequately to the changes in the internal or external environment,
  - Time to begin the cycle again

Maintenance Model

- Focuses on organizational effort on system maintenance:
  - External monitoring
  - Internal monitoring
  - Planning and risk assessment
  - Vulnerability assessment and remediation
  - Readiness and review
  - Vulnerability assessment

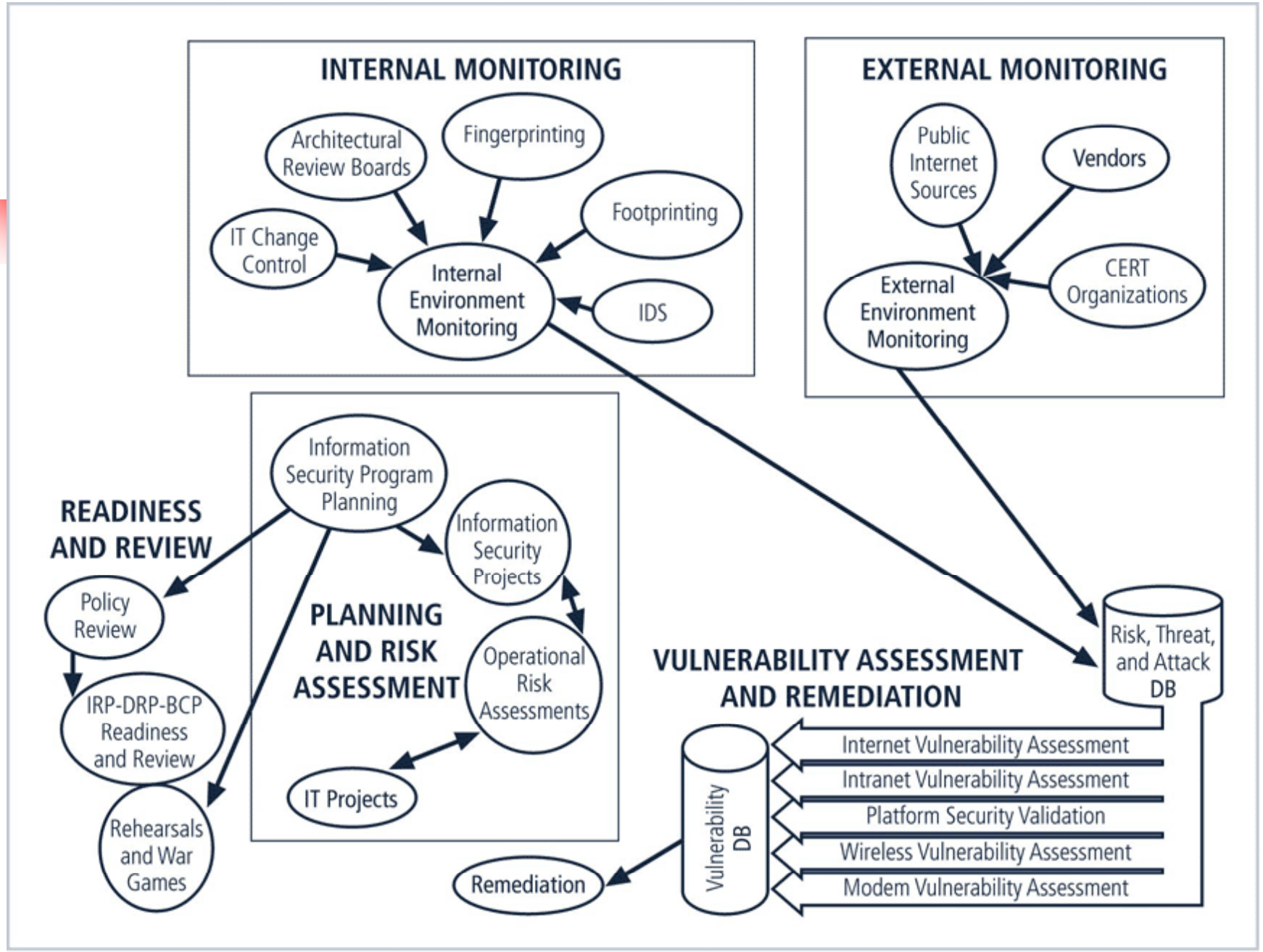
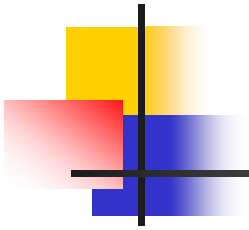
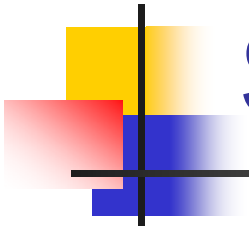


FIGURE 2-10 Maintenance Model



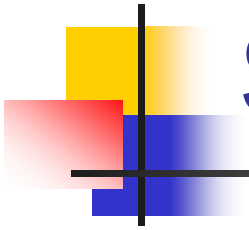
ISO Management Model

- 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 the security program components and administration of changes
- Accounting and Auditing Management
  - involves 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
- Handout
  - Comparison between SDLC and SecSDLC