CSIT988/CSIT488
Security, Ethics and Professionalism
Week 3: Planning for Security

Subject Coordinator: *Guangyou Zhou*

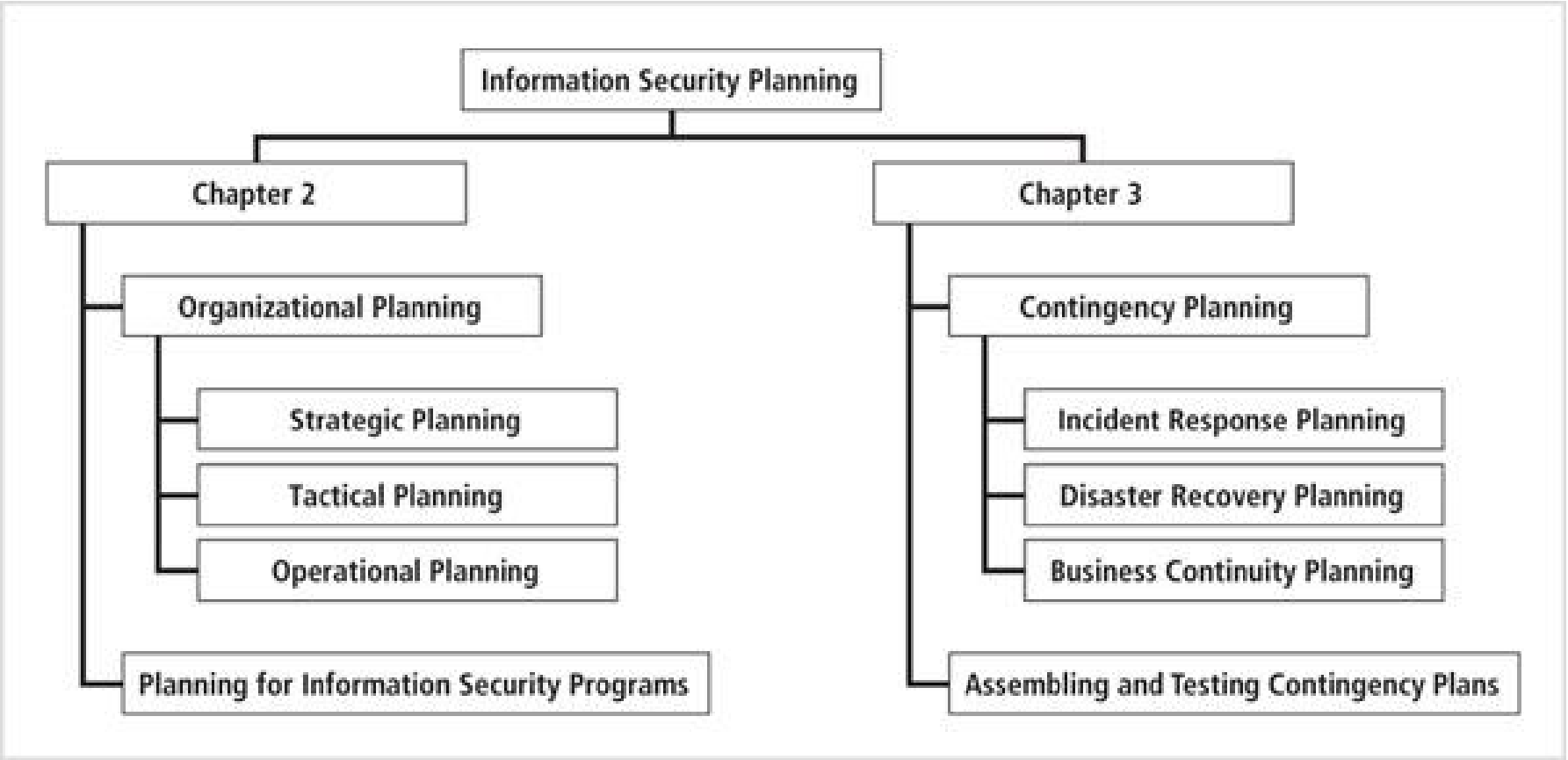
Central China Normal University

Spring 2023

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Week	Lecture Topics	Readings
1	Introduction and overview of the subject	Chapter 1 / No Tutorials
2	Information security management	Chapter 1
3	Planning for security	Chapter 2
4	Planning for contingencies	Chapter 3
5	Information security policy	Chapter 4
6	Developing the security program	Chapter 5
7	Security management models & practices	Chapter 6, 7
8	Risk management: identifying and accessing risk	Chapter 8
9	Risk management: controlling risk	Chapter 9
10	Protection mechanisms	Chapter 10
11	Personnel and security	Chapter 11
12	Law and Ethics	Chapter 12

What Is Planning?



What is planning?

- The process that develops, creates, and implements strategies for the accomplishment of objectives
- Planning is creating action steps toward goals, and then controlling them
- Planning provides direction for the organization's future
- In the top-down method, an organization's leaders choose the direction
  - ➢Planning begins with the general and ends with the specific

What is planning?

- Note that there are differences between leadership and management. A leader influences employees so that they are willing to accomplish objectives. He or she is expected to lead by example and demonstrate personal traits that instill a desire in others to follow. In other words, leadership provides purpose, direction, and motivation to those who follow.
- By comparison, a manager administers the resources of the organization. He or she creates budgets, authorizes expenditures, and hires employees. This distinction between a leader and a manager is important because leaders do not always perform a managerial function, whereas nonmanagers are often assigned leadership roles. However, effective managers are also effective leaders.

Strategic Planning

- **What is Strategic Planning**
  - Strategic planning involves the structured efforts of an organization to effectively identify its purposes for existing, the direction that the organization will pursue, and how that direction will allow the entity to achieve its short-term and long-term goals.
  - Individuals, businesses, governments, non-profit agencies, and any other type of organizations can utilize this process of strategically planning for the future. While the methods used in this type of planning process vary, there are a few basic steps that tend to apply in any setting.

What is planning?

- **What is Tactical Planning**
  - Tactical planning is the step taken after a business or team creates a strategic plan to break that plan into smaller objectives and goals.
  - A tactical plan is used to define goals and determine how they will be achieved through actions and steps. Most tactical plans outline specific steps or actions that will be taken to meet the goals of the larger strategic plan.
  - These actions or steps are then often delegated to the appropriate team members or employees to ensure they are met in a timely fashion.
  - In most cases, tactical planning is implemented when a business or team needs to respond to an immediate issue or situation. For example, a company that wants to win a bid from another business must create a viable proposal that will be successful.

What is planning?

- **What is Operational Planning**
  - Operational planning is a method a department or team uses to take the company's strategic plan and turn it into a detailed map broken up into various components.
  - This map, called the operational plan, documents the team's exact steps within specified time periods to reach each goal. Such a plan is made with a focus on the future to outline budget allocations, departmental activities and targets for the next year to three years.
  - The operational planning meaning becomes clearer when we understand that the operations segment is but one component of a larger strategic plan.
  - In operational planning, it's essential to record each team member's responsibilities for the fiscal year in detail. How detailed the plan is will depend upon the projected timeline for goal completion and how fast the team works.

What is planning? Examples

- **PRODUCTION PLANNING**
  - ➢ This type of operational planning in management is geared towards mapping a business's output. Here the focus is primarily on using labor and capital intelligently to make products that can be sold profitably. Take, for instance, a frozen yogurt manufacturer that creates 10 different flavors within just one facility. Operational planning here will involve organizing supplies and streamlining production lines, work shifts and warehouse space to maintain manageable overhead costs.

What is planning? Examples

- **CAPABILITY PLANNING**
  - Operational planning is required to identify the purpose of a business and then create a roadmap for building on its capabilities. For example, a private taxi company evaluating its own business capabilities will devise a plan to maintain its fleet better and upgrade operations to enhance the safety of women passengers.

What is planning? Examples

- **SALES PLANNING**
  - Operational planning is crucial for matching sales targets with production capabilities. For instance, if a makeup brand wants to run a promotional campaign that could grow sales by 150%, only tight operational planning will be able to determine whether the company's factories can boost production to such a degree.
  - Going over a few key examples of operational planning in management would be helpful to examine how the process actually helps. Let's look at a few benefits of operational planning.

BENEFITS OF OPERATIONAL PLANNING

Without operational planning in management, businesses would run inefficiently and incur losses. Planned operations are a company's lifeblood. Here are some key benefits of operational planning.

- **PROVIDES CLARITY**
  - Among other things, operational planning ensures everyone on the team has a clear idea about the work to be done on a monthly, weekly and even daily basis. This helps maintain focus and increase efficiency.

BENEFITS OF OPERATIONAL PLANNING

Without operational planning in management, businesses would run inefficiently and incur losses. Planned operations are a company's lifeblood. Here are some key benefits of operational planning.

- **PROVIDES A ROADMAP**
  - Achieving long-term goals becomes much easier with operational planning. Productivity increases when team members have a detailed plan to follow; this also helps maintain accountability.

BENEFITS OF OPERATIONAL PLANNING

Without operational planning in management, businesses would run inefficiently and incur losses. Planned operations are a company's lifeblood. Here are some key benefits of operational planning.

- **REDUCES DELAY**
  - With a clearly charted-out path, employees know how much ground they have to cover by the end of each day. This helps them manage their time better and stay on schedule, thereby producing quality and timely work.

The Role of Planning

- Successful organizations utilize planning
- Planning involves
  - Employees
  - Management
  - Stockholders
  - Other outside stakeholders
  - The physical and technological environment
  - The political and legal environment
  - The competitive environment

The Role of Planning

- Strategic planning includes:
  - Values statement
  - 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
- The values, vision, and mission statements together provide the foundation for planning

Values Statement

- Establishes organizational principles and qualities (WHY)
  - ➢ Makes organization's conduct standards clear
    - ✓ *Random Widget Works 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*

Values Statement

UNIVERSITY OF WOLLONGONG AUSTRALIA

Microsoft Values Statement (2013):

- “As a company, and as individuals, we value integrity, honesty, openness, personal excellence, constructive self-criticism, continual self-improvement, and mutual respect. We are committed to our customers and partners and have a passion for technology. We take on big challenges, and pride ourselves on seeing them through. We hold ourselves accountable to our customers, shareholders, partners, and employees by honoring our commitments, providing results, and striving for the highest quality.”

Vision Statement

- The vision statement expresses what the organization wants to become (WHAT)
- Vision statements should be ambitious
  - *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*

Vision Statement

Microsoft's Corporate Vision Statement

Microsoft's corporate vision is "***to help people and businesses throughout the world realize their full potential.***" This vision statement shows that the company presents its business and computing products as tools that people and business organizations can use for their development. Microsoft's corporate vision statement has the following components:

1. People and businesses throughout the world
2. Help to realize
3. Full potential

Mission Statement

Mission statement (HOW)

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

Mission Statement

A mission statement should be

- concise
- should reflect both internal and external operations
- should be robust enough to remain valid for a period of four to six years.

Simply put, the mission statement must explain what the organization does and for whom.

Mission Statement

Microsoft's Corporate Mission Statement

Microsoft's corporate mission is "***to empower every person and every organization on the planet to achieve more.***" This mission statement shows that the business is all about empowerment of people and organizations. Such empowerment is achieved through the utility of the company's computing products. The following components are significant in Microsoft's corporate mission statement:

1. Empowerment
2. Every person and every organization on the planet
3. To achieve more

Mission, Vision and Values Statement

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

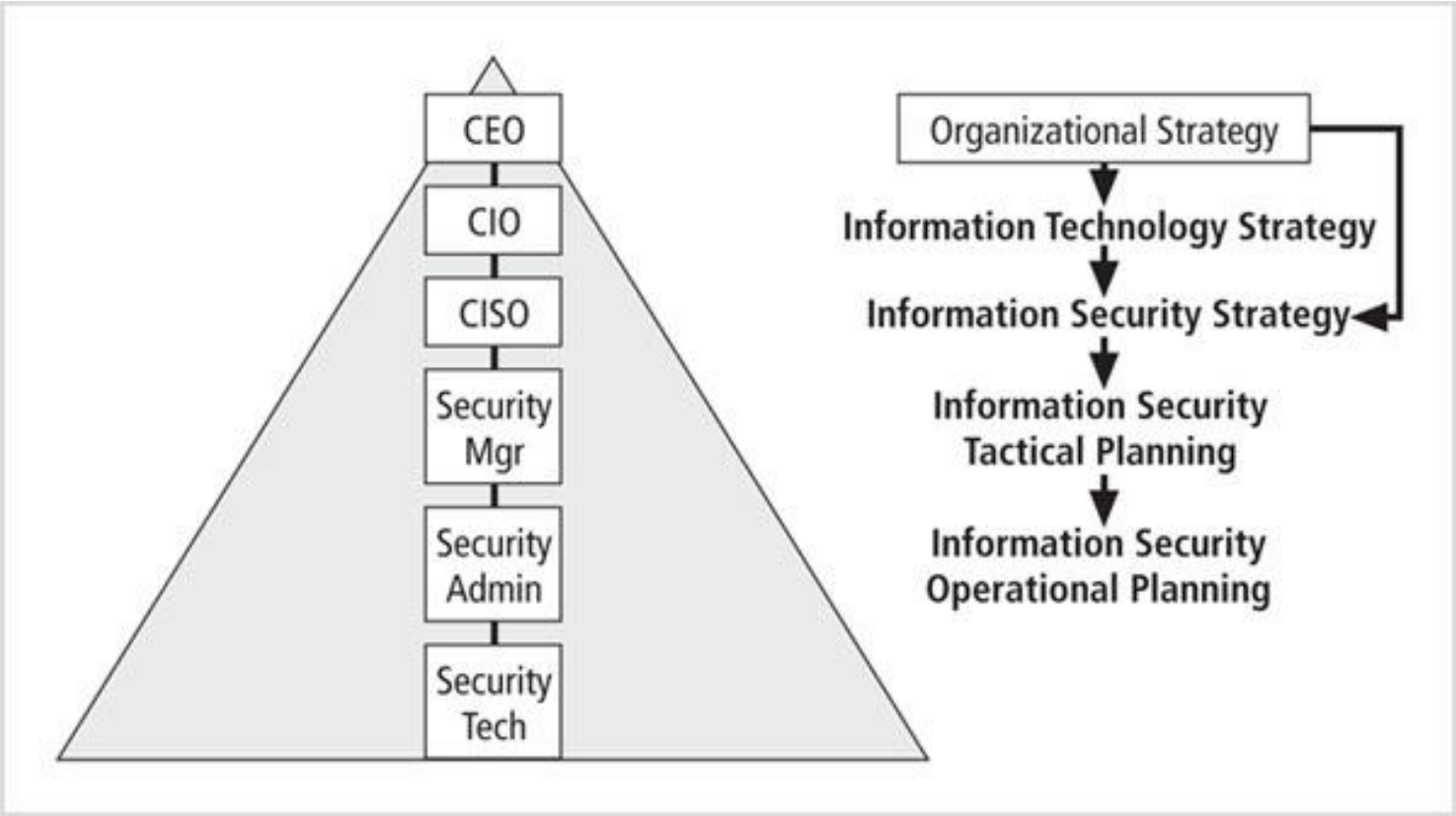
Strategic Planning

- 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

- Strategic plans formed at the highest levels of the organization are translated into more specific strategic plans for intermediate layers of management.
- These plans are then converted into tactical planning for supervisory managers and eventually provide direction for the operational plans undertaken by the nonmanagement members of the organization.
- This multilayered approach encompasses two key objectives: general strategy and overall strategic planning.
- First, general strategy is translated into specific strategy; second, overall strategic planning is translated into lower-level tactical and operational planning.

Creating a Strategic Plan



CEO: Chief Executive Officers
CIO: Chief Information Officers
CISO: Chief Information Security Officers
COO: Chief Operations Officers

Creating a Strategic Plan

- An organization develops a general strategy
  - Then creates specific strategic plans for major divisions
  - Each level or division translates those objectives into more specific objectives for the level below
  - CEO (general statement of strategy): *Providing the highest quality health care service in the industry.*

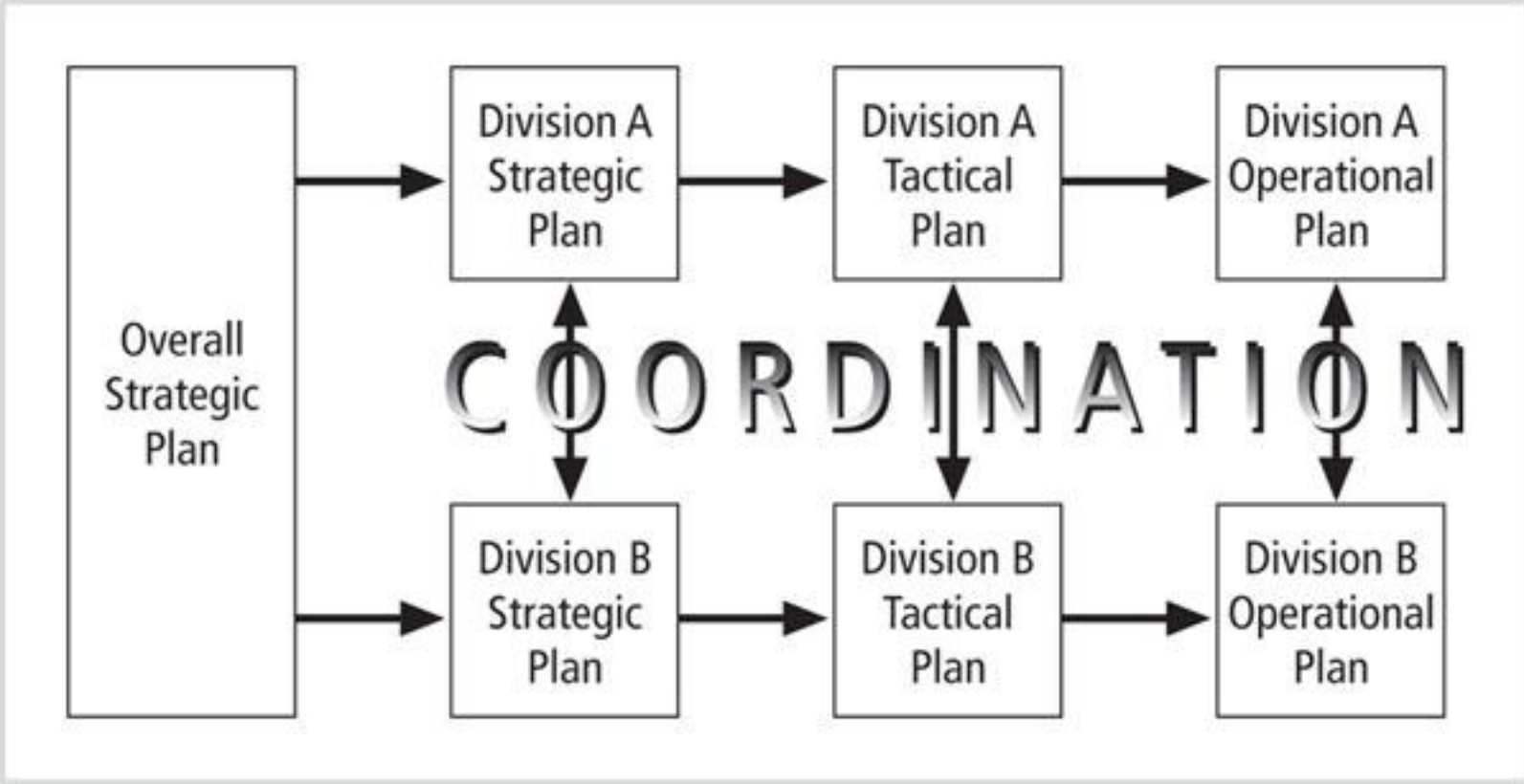
Creating a Strategic Plan

- In order to execute this broad strategy executives must define individual managerial responsibilities
- To response the CEO,
  - CIO: Providing high-level health care information service in support of the highest quality health care service in the industry.
  - COO: Providing the highest quality medical services
  - CISO: Ensuring that quality health care information services are provided securely and in compliance with all local, state, and federal information processing, information security, and privacy statutes, including HIPAA.

Planning Levels

- Strategic goals are translated into tasks
- Objectives should be specific, measurable, achievable, reasonably high and time-bound (SMART)
- Strategic planning then begins a transformation from general to specific objectives
- Strategic plans are used to create tactical plans and then operational plans.

Planning Levels



Planning Levels

- **Tactical Planning**
  - Has a shorter focus (1-5 years) than strategic planning
  - Breaks applicable strategic goals into a series of incremental objectives
  - Each objective should be specific and have a delivery date.
  - Budgeting, resource allocation, personnel are critical components for tactical plan
  - Including project plans, resource acquisition planning documents, project budgets, project reviews, and regular reports.
  - To organize, prioritize and acquire resources to support the overall strategic plan.

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
    - ✓ Associated tasks

Planning and the CISO

- Elements of a strategic plan
  - 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)

Planning and the CISO

- Tips for creating a strategic plan (Brian Ward)
  - 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 the balanced scorecard approach
  - Deploy a draft high level plan early, and ask for input from stakeholders in the organization

Planning and the CISO

- Tips for creating a strategic plan (cont'd.)
  - Make the evolving plan visible
  - Make the process invigorating for everyone
  - Be persistent
  - Make the process continuous
  - Provide meaning
  - Be yourself
  - Lighten up and have some fun

Information Security Governance

- Strategic planning and corporate responsibility are accomplished by using governance, risk management, and compliance (GRC).
- GRC integrate them into one holistic approach for executive-level strategic planning and management.
- Governance of InfoSec is a strategic planning responsibility
  - Importance has grown in recent years
- Information security objectives must be addressed at the highest levels of an organization's management team
  - To be effective and offer a sustainable approach

Information Security Governance

- **Information security governance includes (ITGI)**
  - Providing strategic direction
  - Establishing objectives
  - Measuring progress toward those objectives
  - Verifying that risk management practices are appropriate
  - Validating that the organization's assets are used properly

Information Security Governance

- **Actions of the Board of Directors**
  - Inculcating a culture that recognizes the importance of information security
  - Aligning management's investment in information security with organizational strategies and risk environment
  - Assuring comprehensive development and implementation of an information security program
  - Demanding reports from the various layers of management on the information security program's effectiveness and adequacy

Desired Outcomes

- **Outcomes of information security governance**
  - Strategic alignment of information security with business strategy to support organizational objectives
  - Risk management to reduce potential impacts on information resources
  - Resource management with efficient use of information security knowledge and infrastructure
  - Performance measurement to ensure that organizational objectives are achieved
  - Value delivery by optimizing information security investments in support of organizational objectives

Desired Outcomes

- **Recommended Board of Director practices (National Association of Corporate Directors – NACD, USA)**
  - ➢Place information security on the board's agenda
  - ➢Identify information security leaders, hold them accountable and ensure support for them
  - ➢Ensure the effectiveness of the corporation's information security policy through review and approval
  - ➢Assign information security to a key committee and ensure adequate support for that committee

Benefits of Information Security Governance

- An increase in share value for organizations
- Increased predictability and reduced uncertainty of business operations by lowering information-security-related risks to definable and acceptable levels
- Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care
- Optimization of the allocation of limited security resources
- Assurance of effective InfoSec policy and policy compliance

Benefits of Information Security Governance

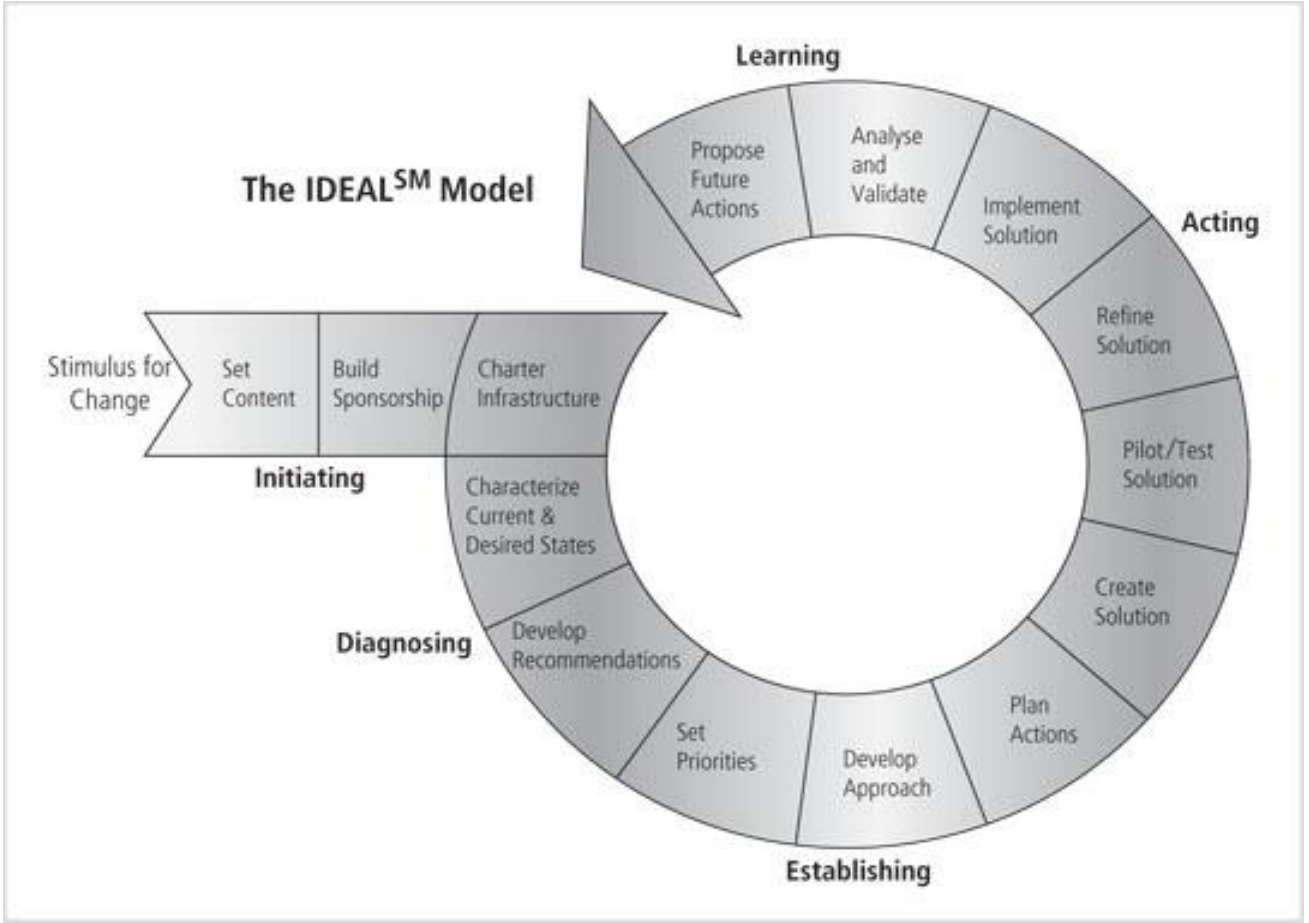
- A firm foundation for efficient and effective risk management, process improvement, and rapid incident response
- A level of assurance that critical decisions are not based on faulty information
- Accountability for safeguarding information during critical business activities, such as mergers and acquisitions,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

Implementing Information Security Governance

I	**Initiating**	Lay the groundwork for a successful improvement effort.
D	**Diagnosing**	Determine where you are relative to where you want to be.
E	**Establishing**	Plan the specifics of how you will reach your destination.
A	**Acting**	Do the work according to the plan.
L	**Learning**	Learn from the experience and improve your ability to adopt new improvements in the future.

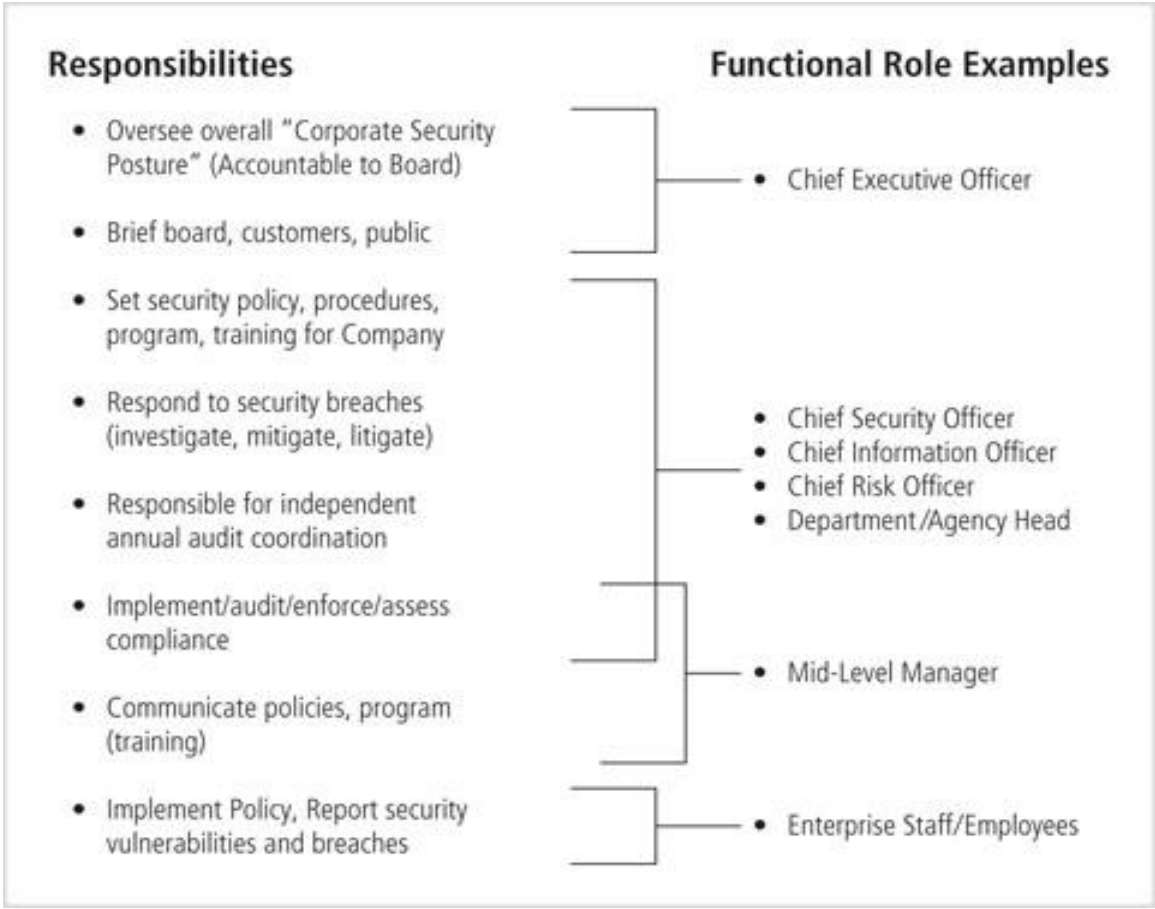
IDEAL model

Implementing Information Security Governance



UNIVERSITY OF WOLLONGONG AUSTRALIA

Planning for Information Security Implementation



UNIVERSITY OF WOLLONGONG AUSTRALIA

Planning For Information Security Implementation

- **Roles of the CIO and CISO**
  - Translating overall strategic plan into tactical and operational information security plans
  - The CISO plays a more active role in the development of the planning details than does the CIO

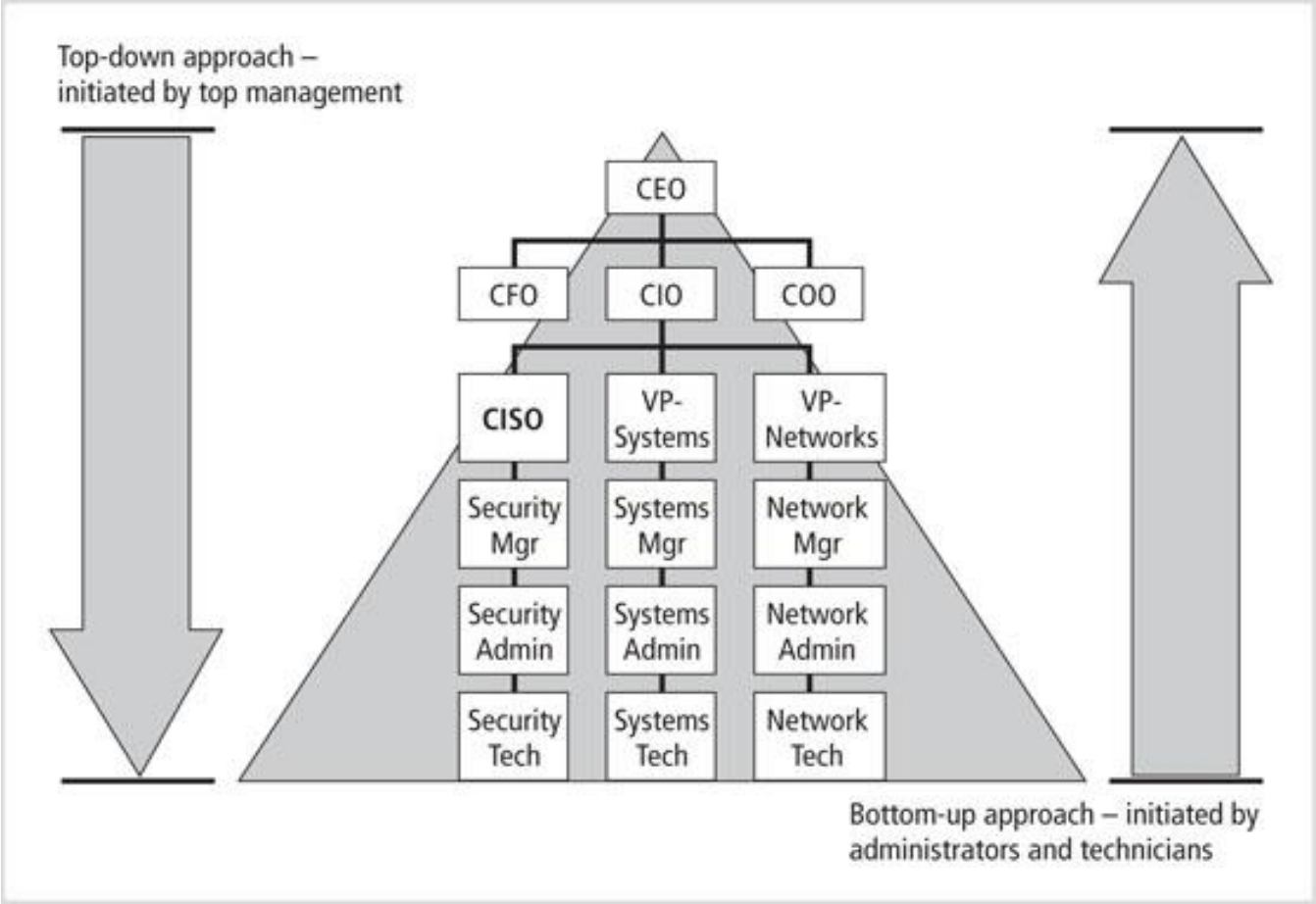
Planning For Information Security Implementation

- **CISO Job Description (example)**
  - Creates a strategic information security plan with a vision for the future of information security
  - Understands the fundamental business activities and suggests appropriate information security solutions to protect these activities
  - Develops action plans, schedules, budgets, and status reports

Planning For Information Security Implementation

- **Implementation can begin**
  - After plan has been translated into IT and information security objectives and tactical and operational plans
- **Methods of implementation**
  - Bottom-up: use technical expertise of the individual. Lack of coordination
  - Top-down: high-level managers provide resources, give direction, issue policies, indicate goals and outcomes, determine responsibilities
  - System development life cycle (SDLC)

Planning For Information Security Implementation



UNIVERSITY OF WOLLONGONG AUSTRALIA

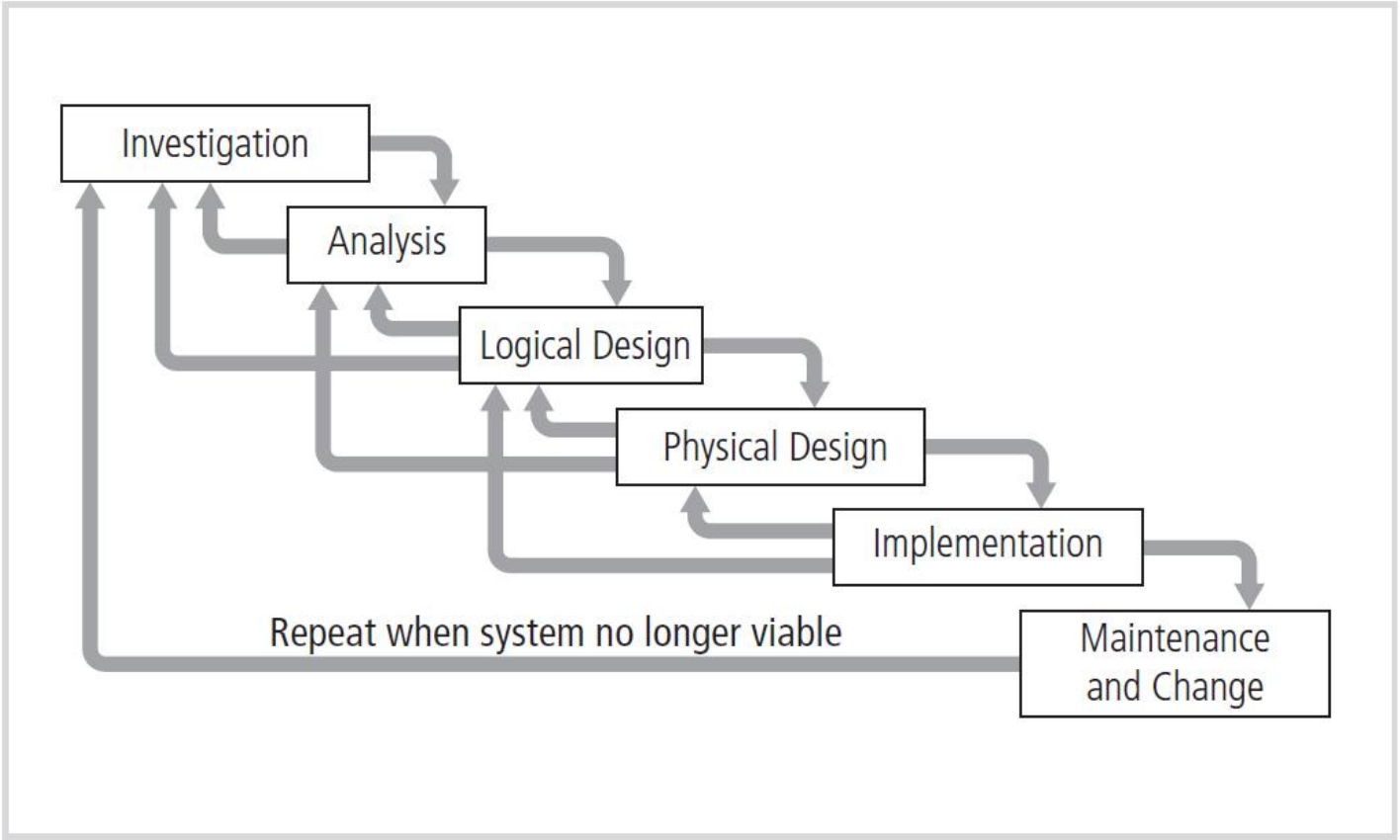
Introduction to the Security Systems Development Life Cycle

- An SDLC is a methodology for the design and implementation of an information system
- SDLC-based projects may be initiated by events or planned
- At the end of each phase, a review occurs to determine if the project should be continued, discontinued, outsourced, or postponed

Introduction to the Security Systems Development Life Cycle

- SecSDLC methodology is similar to SDLC
  - Identification of specific threats and the risks they represent
  - Design and implementation of specific controls to counter those threats and manage risks posed to the organization

Introduction to the Security Systems Development Life Cycle



Investigation in the SecSDLC

- Phase begins with 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 the resources and commitment to conduct a successful security analysis and design

Analysis in the SecSDLC

- Prepare analysis of existing security policies and programs, along with known threats and current controls
- Analyze relevant legal issues that could affect the design of the security solution
- Risk management begins in this stage
  - ✓ The 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
  - ✓ A threat is an object, person, or other entity that represents a constant danger to an asset

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

UNIVERSITY OF WOLLONGONG AUSTRALIA

Threats to information security

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

Threats to information security

- **Some common attacks**
  - Malicious code: virus
  - Hoaxes: false threat
  - Back doors: bypassing access control
  - Password crack: guess a password
  - Brute force: try every possible
  - Dictionary: list of values
  - Denial-of-service (DoS) and distributed denial-of-service (DDoS)

Threats to information security

- **Some common attacks (cont'd.)**
  - Spoofing: unauthorized access
  - Man-in-the-middle
  - Spam
  - Mail bombing
  - Sniffer
  - Social engineering: convince people
  - Buffer overflow
  - Timing: observing the time

Threats to information security

- Prioritize the risk posed by each category of threat
- Identify and assess the value of your information assets
  - ➢Assign a comparative risk rating or score to each specific information asset

Design in the SecSDLC (logical, physical)

- Create and develop a blueprint for security
- Examine and implement key policies
- Evaluate the technology needed to support the security blueprint
- Generate alternative solutions
- Agree upon a final design

Design in the SecSDLC

- Security models may be used to guide the design process
  - 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

Design in the SecSDLC

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

Design in the SecSDLC

- SETA program consists of three elements
  - Security education, security training, and security awareness
- The purpose of SETA is to enhance security by
  - Improving awareness
  - Developing skills and knowledge
  - Building in-depth knowledge

Design in the SecSDLC

- **Design controls and safeguards**
  - Used to protect information from attacks by threats
  - Three categories of controls: managerial, operational and technical
- **Managerial controls**
  - Address the design and implementation of the security planning process, security program management, risk management, and security control reviews

Design in the SecSDLC

- **Operational controls** cover management functions and lower level planning
  - Disaster recovery
  - Incident response planning
  - Personnel security
  - Physical security
  - Protection of production inputs and outputs

Design in the SecSDLC

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

Design in the SecSDLC

- **Contingency planning**
  - Prepare, react and recover from circumstances that threaten the organization
- **Types of contingency planning**
  - Incident response planning (IRP)
  - Disaster recovery planning (DRP)
  - Business continuity planning (BCP)

Design in the SecSDLC

- **Physical security**
  - 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

- **Management of the project plan**
  - Planning the project
  - Supervising the tasks and action steps within the project
  - Wrapping up the project

Implementation in the SecSDLC

- **Members of the development team**
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

Implementation in the SecSDLC

- **Staffing the information security function**
  - Decide how to position and name the security function
  - Plan for the proper staffing of the information security function
  - Understand the impact of information security across every role in IT
  - Integrate solid information security concepts into the personnel management practices of the organization

Implementation in the SecSDLC

- **Information security professionals**
  - Chief information officer (CIO)
  - Chief information security officer (CISO)
  - Security managers
  - Security technicians
  - Data owners
  - Data custodians
  - Data users

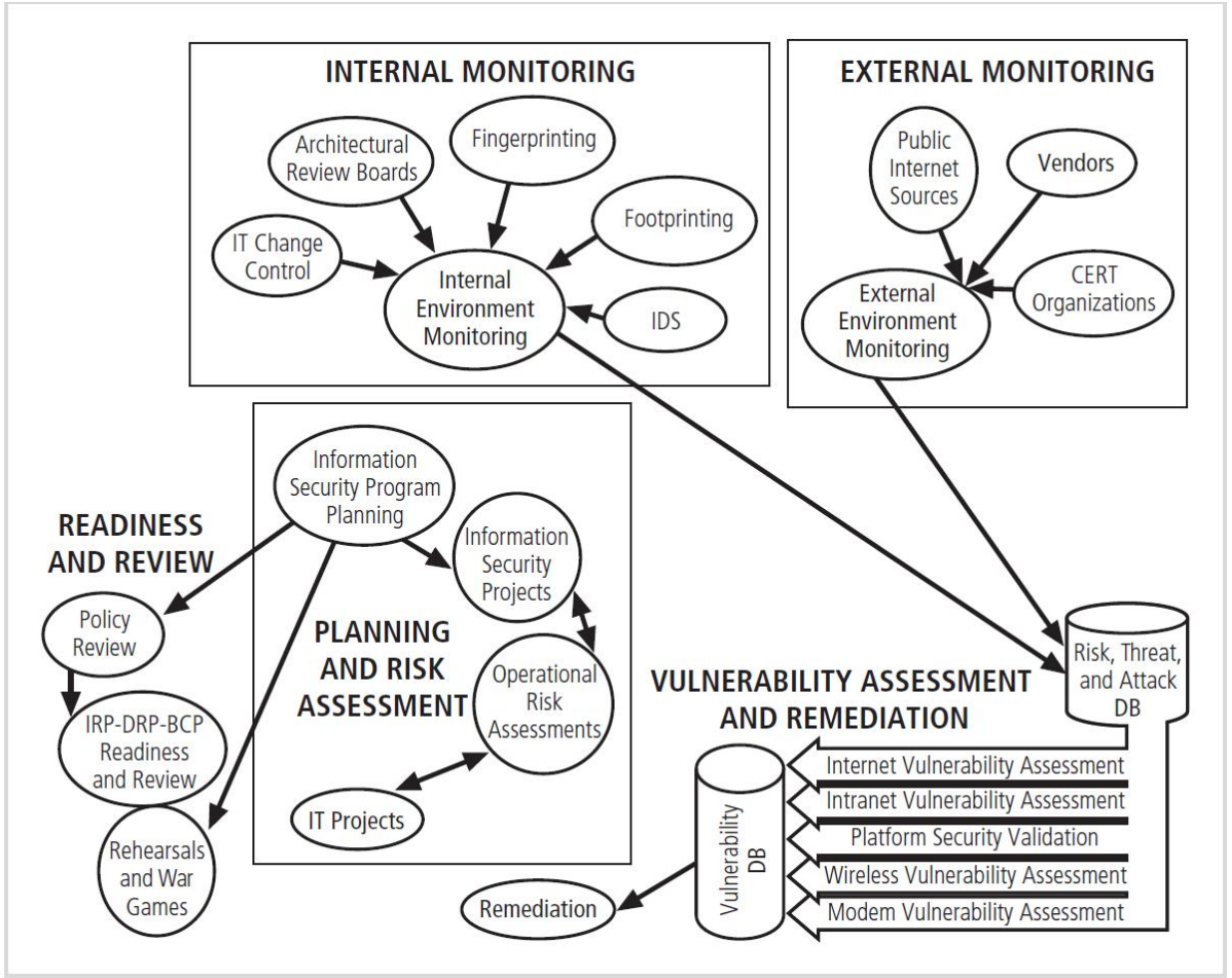
Maintenance and change in the SecSDLC

- Once the information security program is implemented, it must be operated, properly 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 and change in the SecSDLC

- **Aspects of a maintenance model**
  - External monitoring
  - Internal monitoring
  - Planning and risk assessment
  - Vulnerability assessment and remediation
  - Readiness and review
  - Vulnerability assessment

Maintenance and change in the SecSDLC



UNIVERSITY OF WOLLONGONG AUSTRALIA