Lecture 2: Planning for Security

Outline

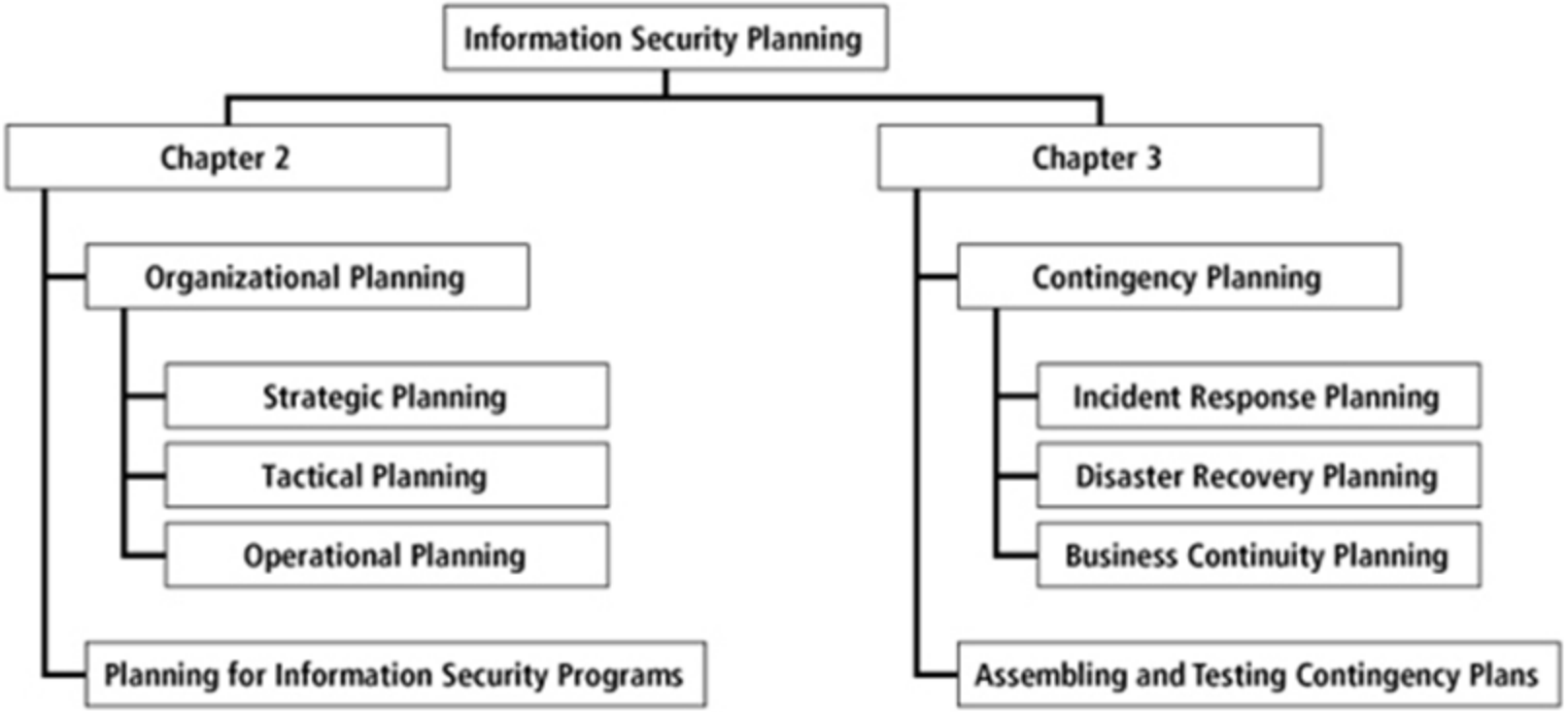
- **2.1 Organizational Planning**
- **2.2 Information Security Governance**
- **2.3 Planning for Information Security Implementation**

Topic 2.1 Organizational Planning

InfoSec Planning

The Process of Planning for InfoSec:

- Compute a path towards InfoSec goals
- Plan for expected and unlikely scenarios



What is planning?

- **Planning** is essential to managing resources
  - provides direction for the organization's future
  - it involves:
    - employees
    - management
    - stockholders
    - outside stakeholders

    groups

    - physical environment
    - political and legal environment
    - competitive environment
    - technological environment

    factors

What is planning?

- **Planning** creates a sequence of actions and then controls them to achieve *specific goals* during a *defined period of time*
  - degree of planning
- **Top-down process**
  - “begins with the general and ends with the specific”
  - organization’s leaders choose the direction
  - first outlines general objectives and then specific detailed objectives
  - creates detailed plans

Why planning?

- **Planning** makes efficient use of resources through coordinated efforts
  - without specific and detailed planning, organizational units would attempt to meet objectives independently
  - good planning enables an organization to make the most out of the materials at hand

Why planning?

- InfoSec community aims to influence the entire organization
  - use the same process and methods as the other two communities
  - knowing how the general organizational planning process works helps the InfoSec planning process
  - utilize resources for long-term visibility of InfoSec program
  - justify the investment: spend too much time, money, and human effort? too little return?
  - balance the benefits of the chosen degree of planning effort against the costs of the effort

Strategic Planning

"… 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."

John Bryson, Strategic Planning in Public and Nonprofit Organizations

Strategic Planning

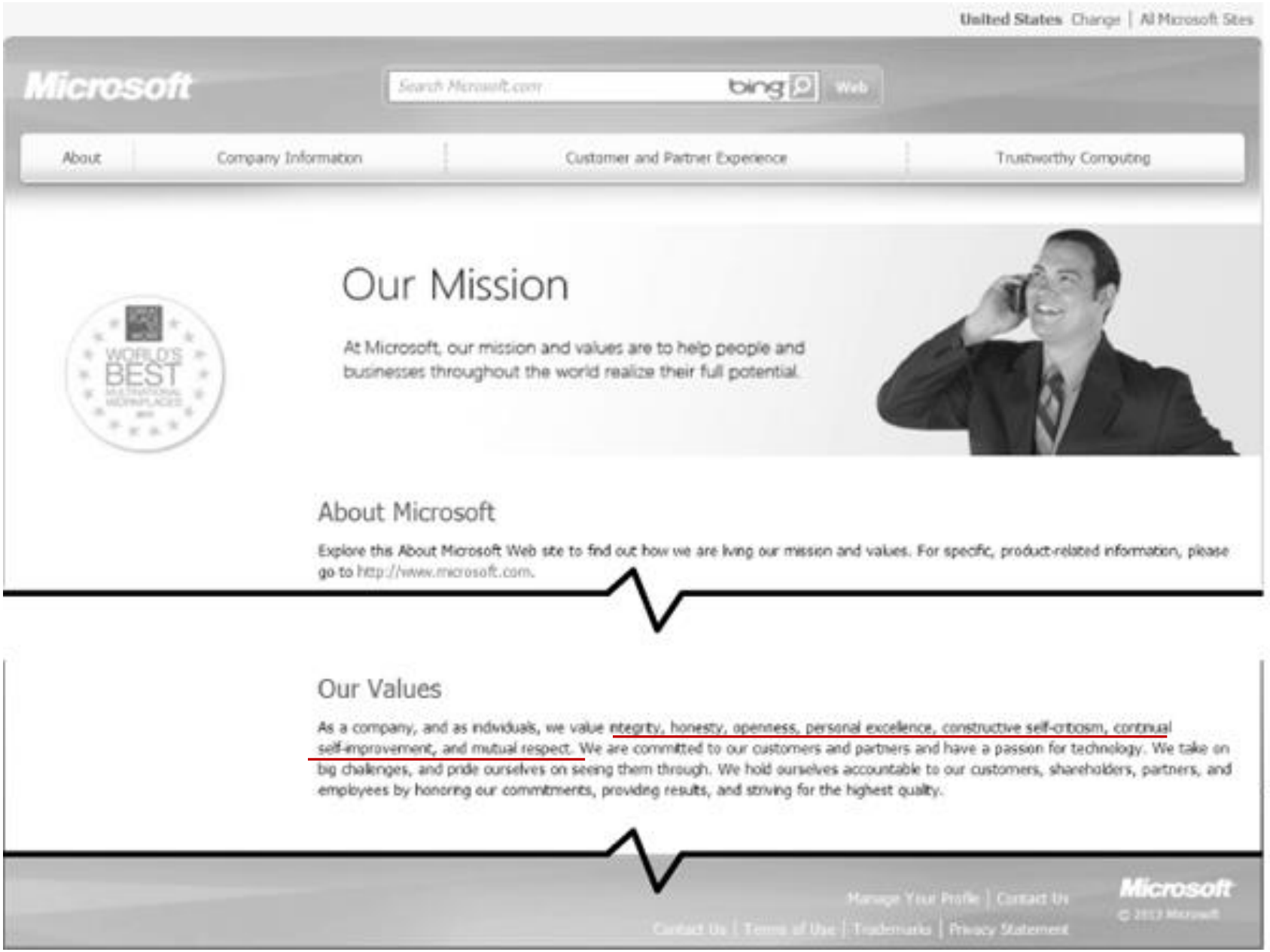
- **Strategic planning** includes:
  - Values statement
  - Vision statement
  - Mission statement
  - Strategy
  - Coordinated plans for sub units

  } foundation of planning

- The values, vision, and mission statements together provide the foundation for planning
  - captures the entrepreneurial, philosophical, and ethical perspectives

Values Statement

- **Values statement** should be one of the *first* positions that management must articulate
  - trust and confidence of stakeholders and the public are important
  - establish ***a formal set of principles and qualities*** in a values statement
  - make organization's *conduct and performance standards* clear to its employees and the public



Source: Microsoft.

Microsoft's mission and values statement

Vision Statement

- **Vision statement** expresses *what the organization wants to become*
  - should be ambitious: best-case scenario for the organization's future
  - not meant to express the probable, only the possible
  - **Example 1:**
    - 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

Mission Statement

- **Mission statement** is the follow-up to the vision statement
  - the vision statement states where the organization wants to go
  - the mission statement describes how it wants to get there
- Note:
  - many organizations mix or combine the vision statement and the mission statement
  - many organizations encourage each division or major department to generate its own mission statement
    - including IT and InfoSec departments

Mission Statement

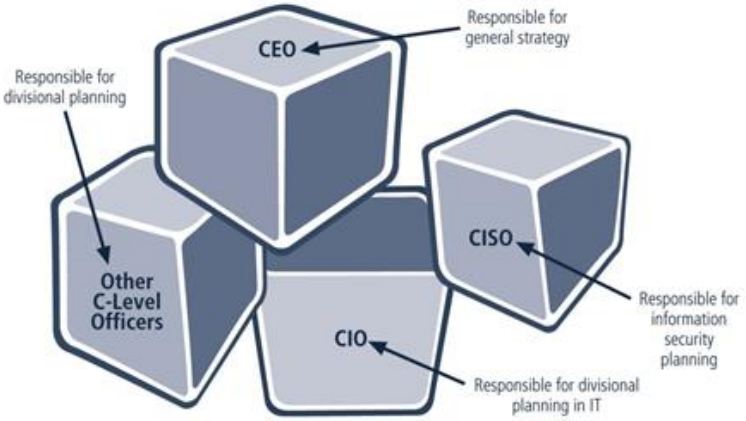
- **Mission statement** explicitly declares the business of the organization and its intended *areas of operations*
  - **Example 2:**
    - Random Widget Works, Inc. designs and manufactures quality widgets and associated equipment and supplies for use in modern business environments
  - be concise
  - reflect both internal and external operations
  - be robust enough to remain valid for a period of four to six years

Problem-based Learning (I)

- **Briefly read the following plans:**
  - Kent county Information Technology Vision and Strategic Plan
  - City of Sarasota Information Technology Strategic Plan
  - ITS Strategic Plan of the University of Idaho
- **Answer the following questions:**
  - Can you find the values statements, vision statements, and mission statements?
  - Discuss why they are important in the strategic plan
    - declare the areas of operations
  - How InfoSec is addressed in the plans?
    - only a component of the plan

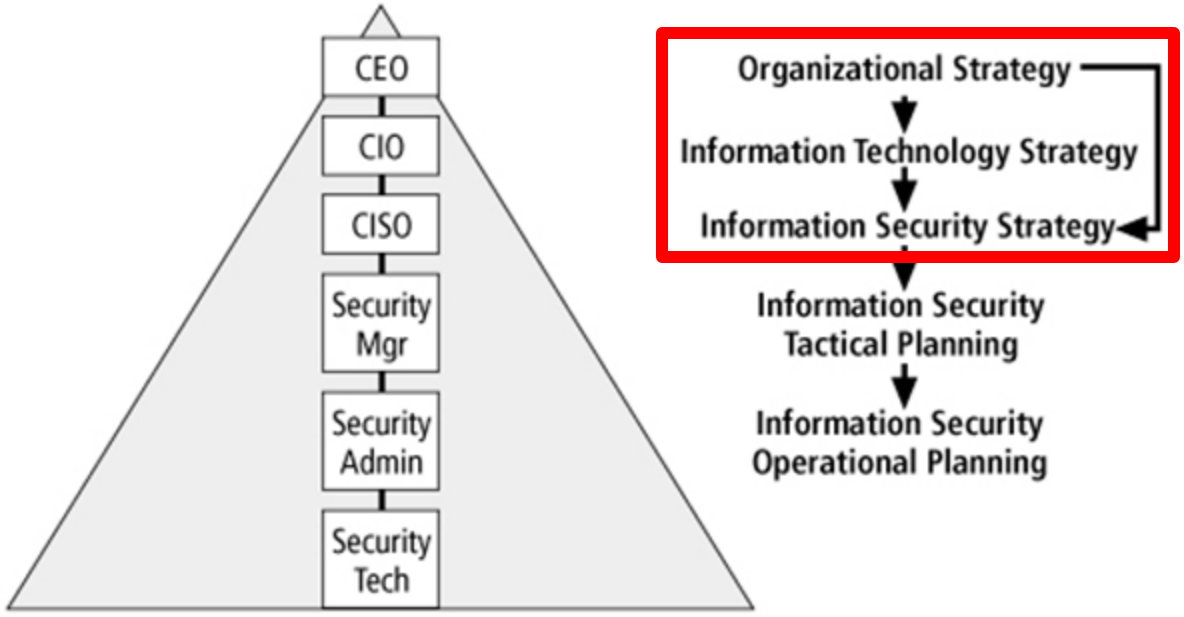
Strategic Planning

- **Strategic planning**
  - lays out the long-term direction
  - guides organizational efforts
  - focuses resources on specific, clearly-defined goals
- **A multilayered approach**
  - creates an overall strategic plan
  - plans for major divisions



Planning Levels: Strategic Planning

- **Top-Down Planning**: strategic plans formed at the highest levels of the organization are translated into more specific strategic plans for intermediate layers of management



Planning Levels: Strategic Planning

Example 3:

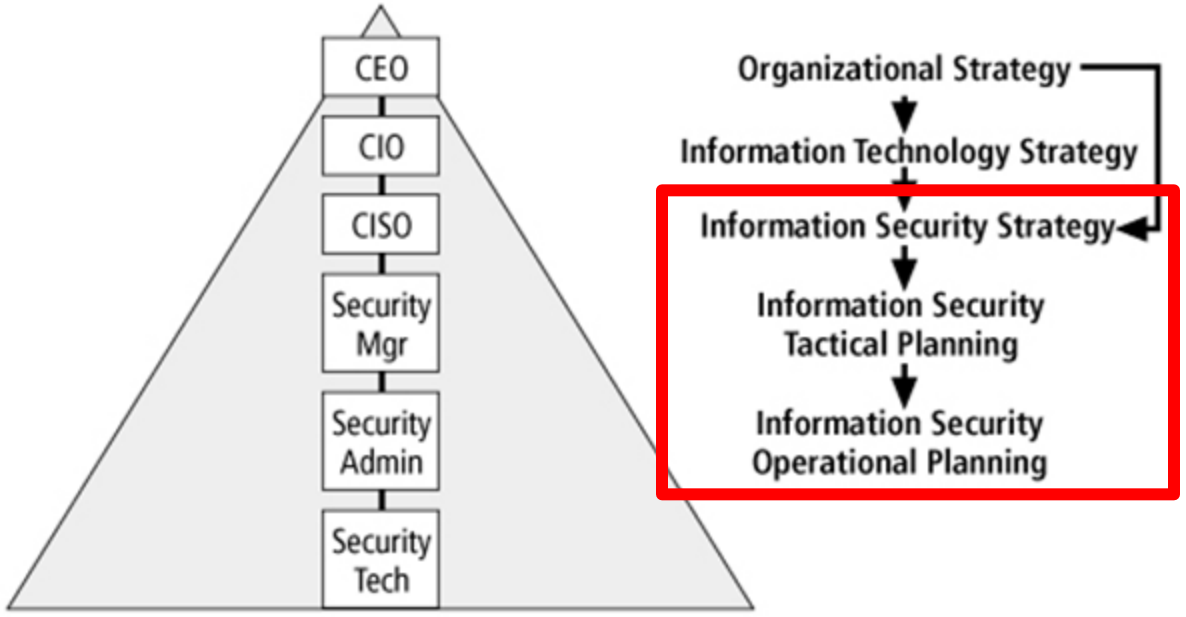
- Providing the highest quality healthcare service in the industry. **CEO**
- Providing the highest quality medical services. **COO**
- Providing high-level healthcare information service in support of the highest quality healthcare service in the industry. **CIO**
- Ensuring that health care information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

Problem-based Learning (II)

- **Read the following security strategic plans:**
  - State of Minnesota Enterprise Security Strategic Plan
  - Metropolitan State University Information Security Plan
  - University of Wisconsin-Madison Information Technology Security Strategy
- **Answer the following questions:**
  - Find the values statements, vision statements, and mission statements
  - Compare them with the ones in IT strategic plans
    - values and vision statements are often missing or expressed less explicitly
    - mission statement, strategies and initiatives are more clear

Planning Levels: Strategic Planning

- **Top-Down Planning**: strategic goals are translated into tasks with specific, measurable, achievable, reasonably high and time-bound objectives (SMART).



Planning Levels: Tactical Planning

- **Tactical planning** has a more *short-term* focus
  - usually 1 to 3 years
  - breaks down strategic goal into a series of incremental objectives (<1 year)
  - budgeting, resource allocation, and personnel are critical components of the tactical plan
- Tactical plans are often created for specific projects
  - a.k.a. process project planning or intermediate planning
  - includes project plans, resource acquisition plans, budgets, project reviews and reports

Planning Levels: Tactical Planning

- **Problem-based Learning (III)**
  - Read State of Minnesota Enterprise Security Tactical Plan
  - Compare with State of Minnesota Enterprise Security Strategic Plan, discuss the difference/focus of two strategic plans at different levels

Planning Levels: Tactical Planning

- **Example 4:** Goal #3 in the information security strategic plan is to "*secure the enterprise network*"
  - What tactical plans can you think of?

Planning Levels: Tactical Planning

- **Example 4:** Goal #3 in the information security strategic plan is to "*secure the enterprise network*"
  - What tactical plans can you think of?
    - define and enforce the network perimeter
    - policies for network usage
    - secure email services
    - secure HTTP services
    - traffic monitoring and intrusion detection
    - ...

Planning Levels: Operational Planning

- Managers and employees use operational plans to organize the ongoing, day-to-day performance of tasks
  - derived from the tactical plans
  - activities, communication requirements, tasks, reports, …
- **Example 5:** Tactical plan includes *"define and enforce the network perimeter"*
  - What is the operational plan?

Planning Levels: Operational Planning

- Managers and employees use operational plans to organize the ongoing, day-to-day performance of tasks
  - derived from the tactical plans
  - activities, communication requirements, tasks, reports, …
- **Example 5:** Tactical plan includes *"define and enforce the network perimeter"*
  - What is the operational plan?
    - design of network topology: selection, configuration, and deployment of switches and bridges
    - selection, configuration, and deployment of a firewall

Planning and the CISO

- Who's responsible?
  - CIO and CISO both play important roles
    - to translate overall strategic planning into tactical and operational information security plans
  - CISO may report directly to the CIO
    - depending on the InfoSec function's placement within the organizational chart
  - CISO plays a more active role in the development of the planning details
  - The first priority of the CISO and InfoSec team should be the structure of a strategic plan

Planning and the CISO

- CISO Job Description
  - Creates strategic InfoSec 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 …

Strategic Security Plan Elements

- A sampling of strategic plans:
  - Organization & Authority Controls
  - Policy
  - Risk Management Program
  - Intelligence Program
  - Audit & Compliance Program
  - Privacy Program
  - Incident Management
  - Education & Awareness Program
  - Operational Management
  - Technical Security & Access Controls
  - Monitoring, Measurement & Reporting
  - Physical & Environmental Security
  - Asset Identification & Classification
  - Employee & Related Account Management Practices

Typical Strategic Plan Components

- Introduction by senior executive (President/CEO):
  - Executive Summary
  - Mission and Vision Statement
  - Organizational Profile and History
  - Strategic Issues and Core Values
  - Program Goals and Objectives
  - Management/Operations Goals and Objectives
  - Appendices (optional)
    - strengths, weaknesses, opportunities and threats (SWOT) analyses, surveys, budgets, etc.

Topic 2.2 Information Security Governance

Information Security Governance

- **Example 6:** Organization's new goal is to support employees to work from remote (home).
  - What's the impact on information security planning?
    - VPN?
  - Cannot achieve organization's new goal without a well designed and implemented security plan.
- **Example 7:** Conventional retail stores keep billions of credit card and transaction records
  - Policies and resources to secure such information
  - What if the information is leaked?
  - Risk management and incident response are needed: at corporate level.

Information Security Governance

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

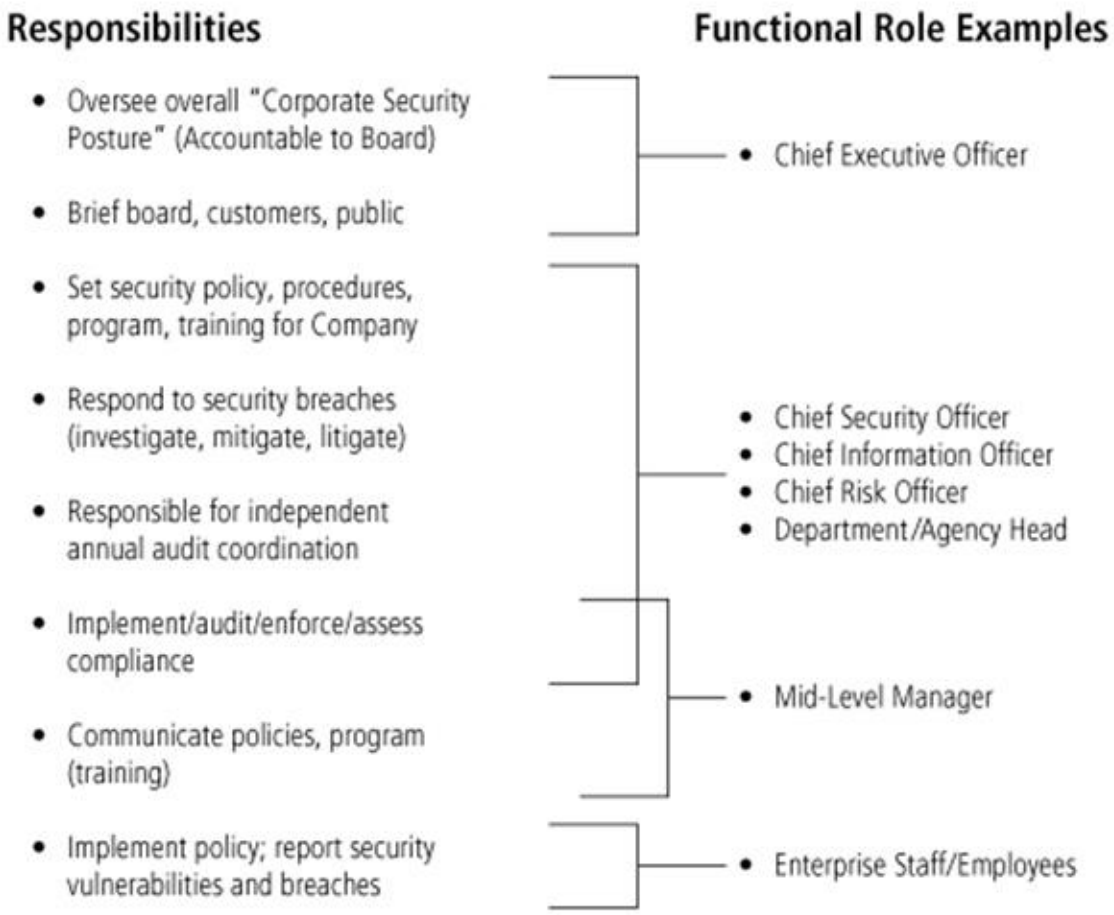
Information Security Governance

As defined by ITGI (Info Tech Governance Institute):

InfoSec governance includes all the accountabilities and methods undertaken by the *board of directors* and executive management to provide:

- strategic direction
- establishment of objectives
- measurement of progress toward objectives
- verification that risk management practices are appropriate
- validation that assets are used properly

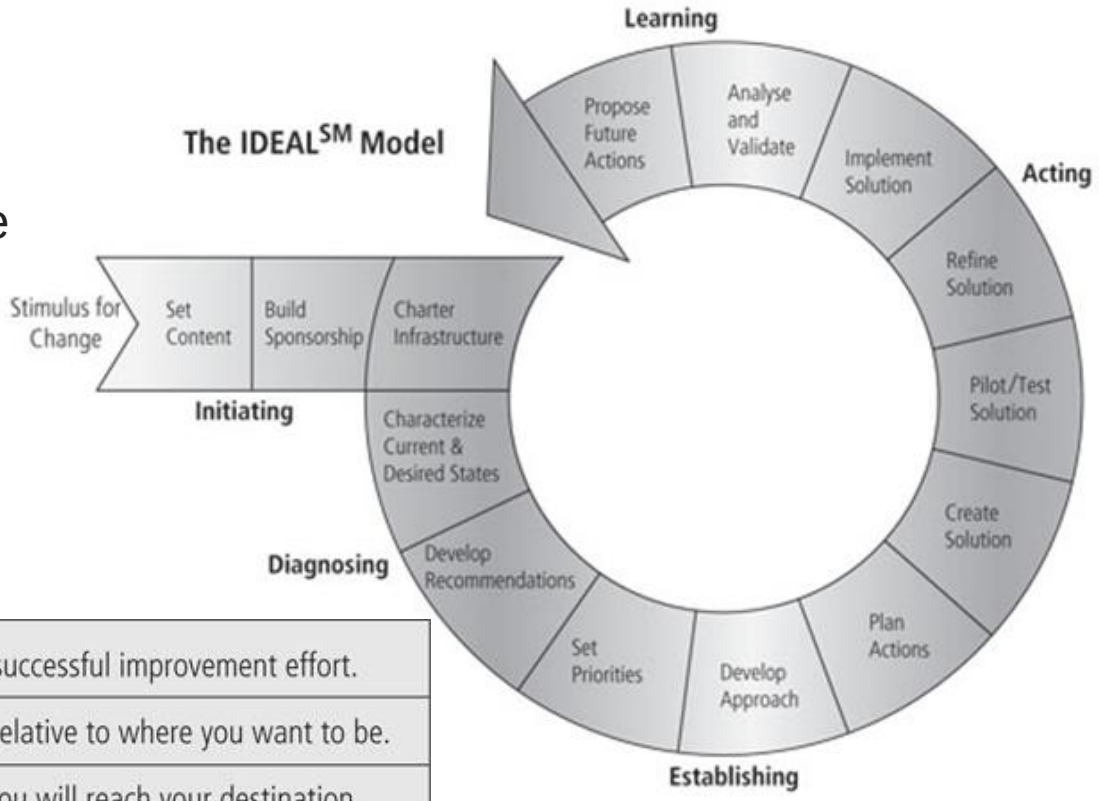
Responsibilities of Functional Roles



IDEAL^{SM} Governance Framework

Developed by CMU SEI

Recommended by Corporate Governance Task Force



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.

Implementing InfoSec Governance

- How to implement effective security governance?
- Core set of activities:
  1. Conduct an annual InfoSec evaluation, reviewed by CEO and reported to the board of directors
  2. Conduct periodic risk assessments of information assets
  3. Implement policies and procedures based on risk assessments to secure information assets
  4. Develop and implement incident response procedures
  5. Establish plans, procedures, and tests to provide continuity of operations

Implementing InfoSec Governance

6. Establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability
7. Treat InfoSec as an integral part of the system
8. Develop plans and initiate actions to provide for adequate InfoSec
9. Provide InfoSec awareness, training, and education
10. Conduct periodic testing and evaluation of the effectiveness of InfoSec policies and procedures
11. Create and execute a plan for remedial action to address any InfoSec deficiencies
12. Use security best practices guidance

Desired Outcomes

- Five outcomes of InfoSec governance:
  - Strategic alignment of InfoSec with business strategy to support organizational objectives
  - Risk management by executing appropriate measures to manage and mitigate threats to information resources
  - Resource management by utilizing InfoSec knowledge and infrastructure efficiently and effectively
  - Performance measurement by measuring, monitoring, and reporting InfoSec governance metrics to ensure organizational objectives are achieved
  - Value delivery by optimizing InfoSec investments in support of organizational objectives

Benefits of InfoSec Governance

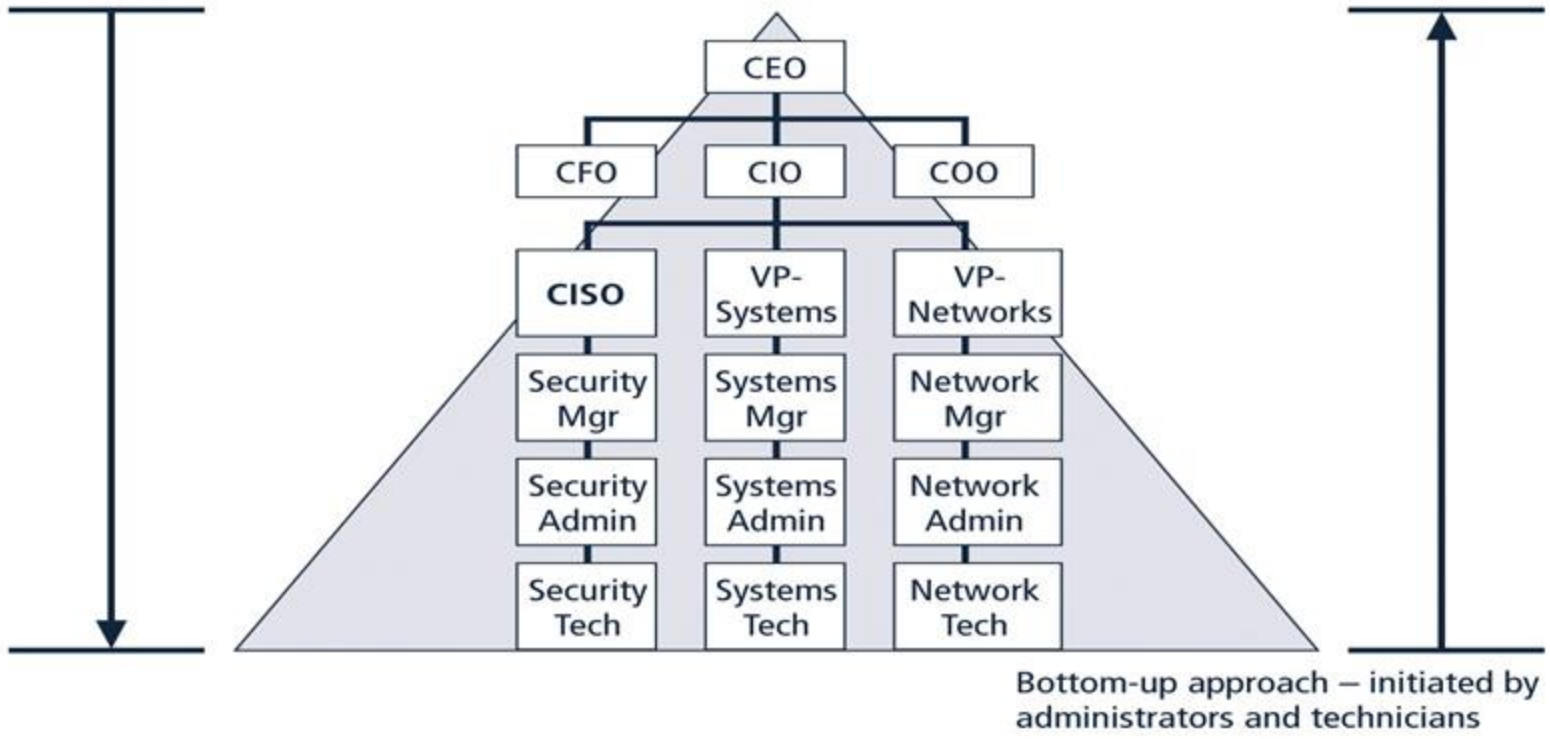
- Benefits, if properly implemented, include:
  - Optimization of the allocation of limited security resources
  - Assurance of effective InfoSec policy and policy compliance
  - An increase in share value for organizations
  - Increased predictability & reduced uncertainty of business operations
  - Protection from increasing potential for civil or legal liability
  - A level of assurance that critical decisions are based on correct info
  - Accountability for safeguarding info during critical business activities
    - e.g., mergers and acquisitions, business process recovery, and regulatory response
  - A firm foundation for efficient and effective risk management, process improvement, and rapid incident response

Topic 2.3 Planning for Information Security Implementation

Approaches to Security Implementation

- Two ways:

Bottom-up LACKS coordinated planning from upper management, coordination between departments and provision of resources.



SecSDLC

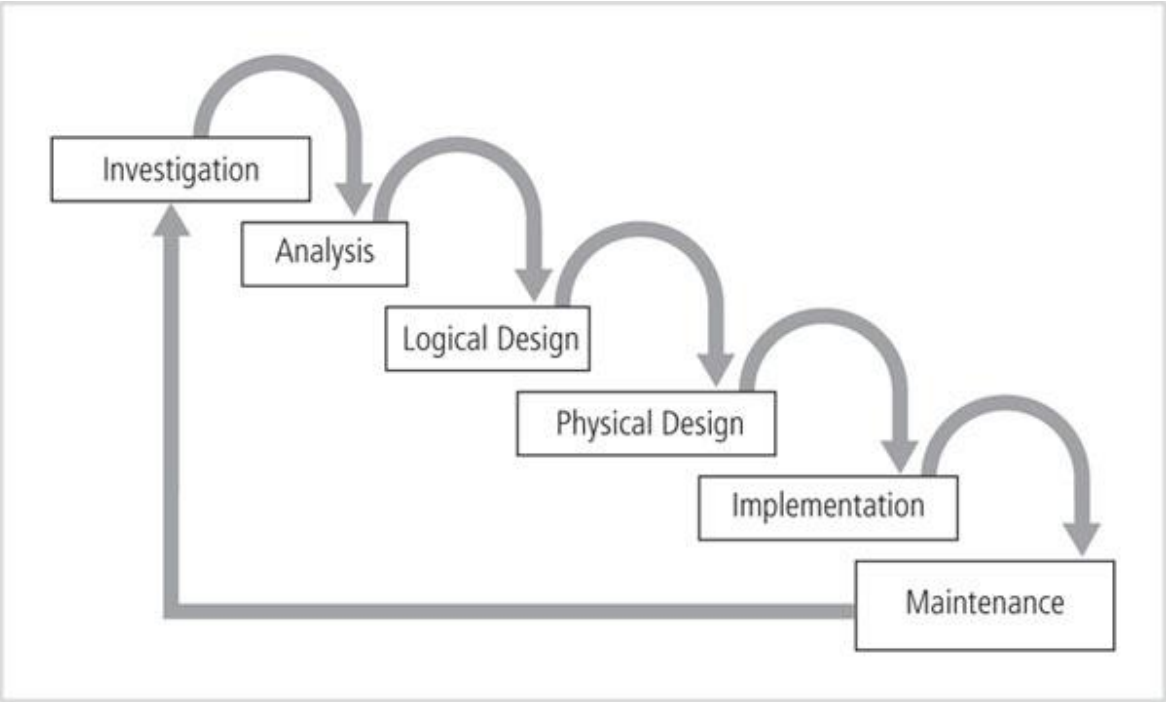
- **Security Systems Development Life Cycle**
  - a most successful top-down approach
  - incorporates a formal development strategy – **SDLC**
    - **SDLC** is a methodology for the design and implementation of an information system
    - a formal approach to solving a problem based on a structured sequence of procedures
    - ensures a rigorous process and increases the likelihood of achieving the desired final objective
    - e.g., waterfall, spiral, evolutionary, agile development, rapid application development

SecSDLC

- SDLC-based projects can be
  - **plan-driven**: the result of a carefully developed planning strategy
  - **event-driven**: a response to some event
    - in the business community, inside the organization, or within the ranks of employees, customers, or other stakeholders
  - a **structured review** (reality check) takes place at the end of each phase
    - to decide if project should be continued, outsourced, or postponed

SecSDLC

- **SecSDLC** methodology is similar to SDLC
  - identification of specific threats and associated risks
  - design and implementation of specific controls to counter those threats and manage risks posed to the organization



Investigation in the SecSDLC

- **Directive** from upper management specifies the process, outcomes, and goals of the project as well as budget and other constraints
- **Teams** of managers, employees, consultants are assembled to:
  - investigate problems
  - define their scope
  - specify goals and objectives
  - identify any additional constraints not covered in security policy
- Conduct organizational **feasibility analysis** to determine if there are resources and commitment

Problem-based Learning

- A nation-wide retail chain, TarMart, stores its transaction data in seven regional data centers
  - Terminals at stores could only connect to their corresponding local data centers
  - At the request of terminals, a data center may query other data centers to access remote transaction data, e.g., when a customer buys a product in California and returns it to New Hampshire
- Event: one of the data centers was recently hacked
  - Attacker impersonated the Northeast data center, and requested a large amount of credit card information from Pacific data center

Problem-based Learning

- The senior management team of the corporate decided to improve data security
- Among several initiatives, the **Locker Project** is to construct a centralized archival data center (the Locker) – 1 year after creation, records will be moved from regional data centers to the Locker
- Some expectations from upper management:
  - Batch data transportation to the locker. Data transportation must be very secure. During data transportation, regional centers could only write to the locker – they cannot read from the locker
  - Only higher-ranked employees could read from the locker
  - Only a very small amount of data could be read from the locker in each request

Problem-based Learning

- You, as the CISO of TarMart, are charged to design the security system for the Locker
- Group discussion:
  - What will you achieve in the investigation phase?
    - give a sample problem
    - the scope of the problem
    - to tackle the problem, what are the goals and objectives?
    - what are possible constraints not (currently) identified in the enterprise security policy?

Analysis in the SecSDLC

- Team studies documents from investigation phase
  - conduct a preliminary analysis of existing security policies
  - conduct an analysis of relevant legal issues that could affect the design of the security solution
  - **risk management**: identifying, assessing, and evaluating the levels of risks
    - specifically threats to the organization's security and to the information stored and processed
    - a **threat** is an object, person, or other entity that represents a constant danger to an asset

Threats to Information Security

12 general categories represent real and present dangers

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

Key Terms

- **Vulnerability:** an identified weakness of a controlled information asset in which necessary controls are not present or inadequate
- **Exploit:** a technique or mechanism used to compromise an information asset
- **Attack:**
  - Technical attack is an act that exploits a vulnerability to achieve the compromise of a controlled information asset
  - There are non-technical attacks that result from natural event or less sophisticated approaches
  - Accomplished by a threat agent that damages or steals an organization's information or physical asset

Some Common Attacks

Password crack/Brute force/Dictionary
Back doors
Buffer overflow
Malicious code
Hoaxes
Denial-of-service (DoS)
Distributed denial-of-service (DDoS)

Spoofing
Sniffer
Man-in-the-middle
Timing
Spam
Mail bombing
Phishing
Social engineering

Analysis in the SecSDLC

- **Risk management** is part of the analysis phase
  - identifies vulnerabilities in an organization's information systems
  - takes steps to assure confidentiality, integrity, and availability of information systems
- Once threats identified, an organization should assess the risk for each of the information assets via
  - **Risk Analysis**: analyzes the related vulnerabilities of the organization's information assets to the threats
  - or **Risk Assessment**: assigns a comparative risk rating or score to each specific information asset

Problem-based Learning

- You, as the CISO of TarMart, are charged to design the security system for the Locker.
- Group discussion:
  - What will you do in the analysis phase?
    - Discuss the following threats: human error, hardware failure, unauthorized data access
    - For each threat: please assess the risk, please discuss possible mitigation approaches.

Design in the SecSDLC

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

Design in the SecSDLC

- **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
  - **InfoSec policies**
    - A critical design element of the InfoSec program
    - It provides rules for the protection of information assets
    - Management must define three types of security policy
      - General or enterprise InfoSec policy (EISP)
      - Issue-specific security policies (ISSP)
      - Systems-specific security policies (SysSP)

Design in the SecSDLC

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

Design in the SecSDLC

- The design phase continues with the formulation of **controls** and **safeguards** used to protect information
- **Three categories** of controls:
  - Managerial controls: cover security processes that are designed by the strategic planners
    - Set the direction and scope of the security process
    - Also address the design and implementation of
      - Security program management
      - Risk management
      - Security control review
      - Legal compliance and maintenance of the entire security life cycle

Design in the SecSDLC

- The design phase continues with the formulation of **controls** and **safeguards** used to protect information
- **Three categories** of controls:
  - Operational controls: deal with the operational functionality of security in the organization
    - Cover tactical management functions and lower-level planning
      - Disaster recovery
      - Incident response planning
      - Personnel security
      - Physical security
      - Protection of production inputs, outputs
      - Development of SETA
      - Hardware, software maintenance

Design in the SecSDLC

- The design phase continues with the formulation of **controls** and **safeguards** used to protect information
- **Three categories** of controls:
  - Technical controls: address technical approaches used to implement security
    - Logical access control: identification, authentication, authorization, accountability
    - Must be integrated into the IT structure

Design in the SecSDLC

- **Contingency plans**
  - Overall planning to prepare for, react to, and recover from events that threaten security of information assets in the organization
  - Creation of essential preparedness documents for
    - Disaster Recovery Planning (DRP)
    - Incident Recovery Planning (IRP)
    - Business Continuity Planning (BCP)

Design in the SecSDLC

- **Physical security**
  - Require 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

- During the implementation phase:
  - Security solutions are acquired, tested, implemented, and re-tested
  - Personnel issues are evaluated
  - Specific training and education programs are conducted
  - Entire tested package is presented to upper management for final approval
- A most important element of this phase is the management of the project plan
  - Planning the project
  - Supervising tasks and action steps within the project
  - Wrapping up the project

Implementation in the SecSDLC

- **InfoSec project team**
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - System administrators
  - End users
- **Staffing** – address human resource issues
  - decide how to position and name the security function, and plan for proper staffing for the InfoSec function
  - understand how InfoSec affects every role in IT, and integrate solid InfoSec concepts into personnel management practices

Maintenance in the SecSDLC

- InfoSec program must be operated, properly managed, and kept up-to-date
  - constant monitoring, testing, modifying, updating, and repairing
  - address deficiencies and vulnerabilities