INFO6027
Information Security Planning

Week 8: Planning for Security

FANSHAWE

Housekeeping

- Any questions about **Assignment #2**?

- Test **week 10** (Wednesday Nov 15 at 12 00 Noon EST)
  - If this doesn’t work for you, AND you are studying outside EST or are a part time student, email me so we can work out an alternate time for you to write.
  - Content from lecture slides, tutorial discussions, assignments, and textbooks
  - Be ready for all kinds of questions, short and long answer, t/f, mc, FIB, matching, scenarios. **Time management during tests is important**

- **ISM2 Elective courses**
  - Go to ISM homepage on FOL

Agenda for Week 8

- BOM – Business Operations Management
- Mission, Vision, and Value Statements
- Strategic Plans, Planning Levels
- **Governance**
- Security Programs like **SecSDLC**
  - Security System Development Life Cycle
    - CISSP Domain 8: Software Development Security (about 10% of CISSP exam)
    - We will **explore all 6 phases**
- Discussion Forum Ideas, Summary, and Reminders

Groups Assemble!!

In this week's discussion forum, please answer the following guiding questions for this lesson

1. **What is the difference between strategic, operational, and tactical plans?**

2. **Choose any company (not Fanshawe College) and try to find that company's mission, vision, and values statements online. Share the link(s). Are these well-written?**

3. **What is the balanced scorecard (BSC) framework?**

4. **Define governance. What is it and how does it apply to Security Planning?**

5. **Explain the difference between top-down and bottom-up management?**

6. **What is the SDLC? Is it different from the Security Systems development life cycle?**

7. **What is the waterfall model of SDLC?**

FANSHAWE

Introduction

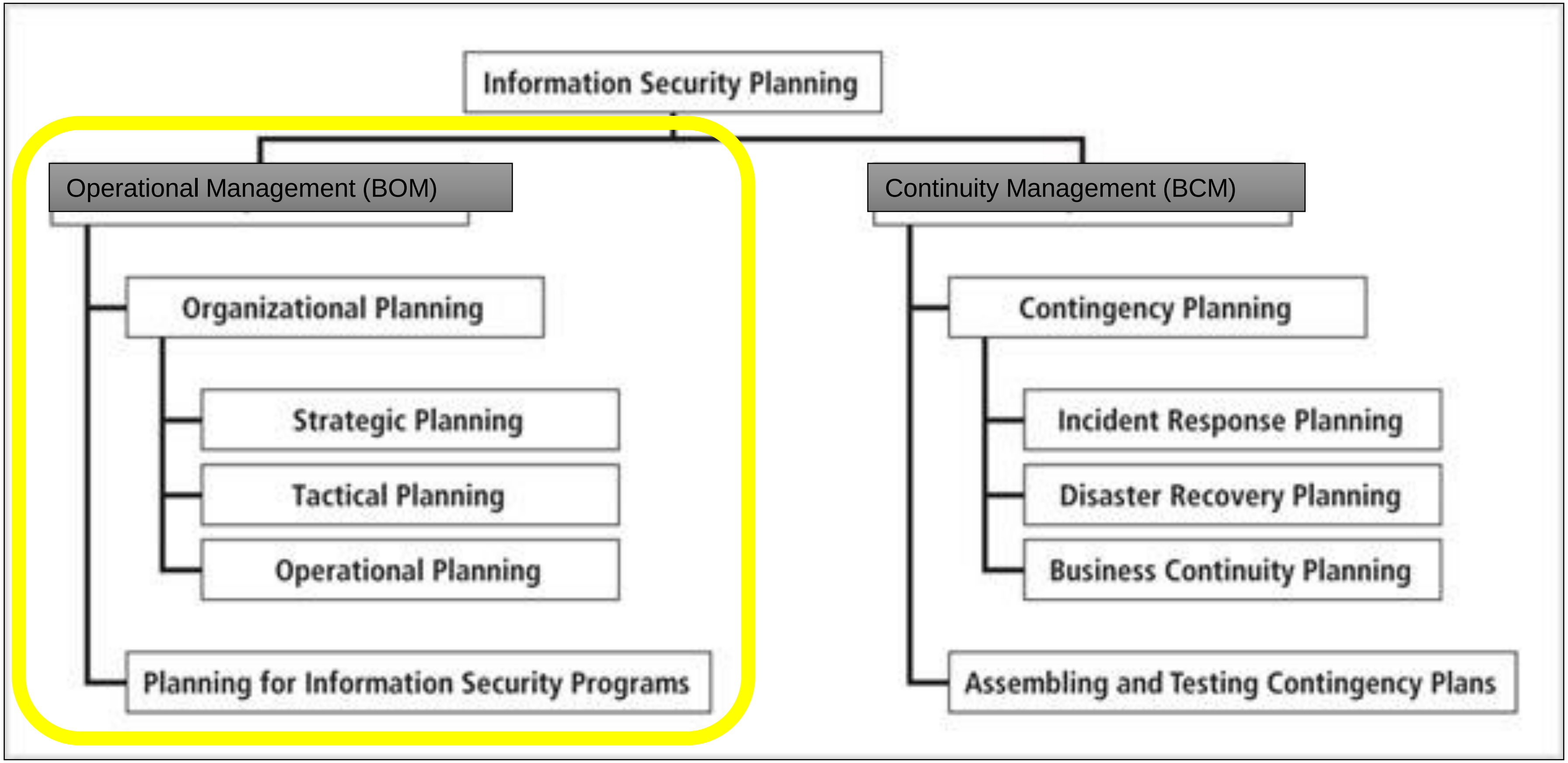

Information Security Planning
Operational Management (BOM)
Continuity Management (BCM)
Organizational Planning
Strategic Planning
Tactical Planning
Operational Planning
Planning for Information Security Programs
Contingency Planning
Incident Response Planning
Disaster Recovery Planning
Business Continuity Planning
Assembling and Testing Contingency Plans

Figure 2-1 Information Security and Planning

Source: Course Technology/Cengage Learning

Review: What is Planning?

- Planning is *creating action steps toward ________.*
- Planning provides direction for the organization’s future
- In the top-down method, an organization’s leaders choose the direction
  - This direction represents the organization's ethical, entrepreneurial and philosophical perspectives
- Planning usually begins with the **general** and ends with the **specific**
- Successful organizations utilize planning
  - They aren’t always reacting or caught **unprepared**

Who is involved in Planning?

- Planning involves/includes
  - Employees
  - Management
  - Stockholders
  - Other outside stakeholders
  - The physical and technological environment
  - The political and legal environment
  - The competitive environment
- Knowing how the **general** organizational planning process works helps in the **information security** planning process
- *How do we decide what we plan for?*

Types of Plans

1. Strategic planning includes:
   - ✓Vision statement
   - ✓Mission statement
   - ✓Strategy
   - ✓Coordinated plans for sub units
   - ✓Usually LONG TERM goals (3-5 years)
2. Tactical Planning
   - ✓ Takes a company's strategic plan and creates specific short-term actions and plans (in the next 1-2 years)
   - ✓ Usually at a department level (or function-based).
3. Operational Planning
   - ✓ Planning for what happens daily, weekly, monthly
   - ✓ How the organization needs to run daily to meet it's strategic goals

Type 1: Strategic Planning

VISION
MISSION
VALUES
STRATEGY

Strategic Planning

- Is guided by the organization's Mission, Vision, and Values statements. These provide the philosophical foundation for all organizational planning.
- https://www.google.com/about/philosophy.html
- Lays out long-term direction for the organization
- Guides organization efforts. Provides **direction**.
- Focuses resources towards specific, clearly defined goals
- Create trickle-down effect on **tactical** and **operational** plans

Strategic Plan: Mission Statement

- Mission statement
  - Follow-up to the Vision Statement (where you want to go)
  - Declares the business of the organization and its intended areas of operations (what it does and for whom to attain the vision)
  - Explains what the organization does and for whom

  For example: *Random Widget Works, Inc. designs and manufactures quality widgets and associated equipment and supplies for use in modern business environments*

Mission Statements should be short/concise and generally worded to the point where it will be **applicable for 4-6 years**

Strategic Plan: Vision Statement

- The vision statement ***concisely*** expresses what the organization **wants to become**
- Vision statements should be ambitious! **Why?**
  - Don't worry about probable…think possible
  - Should **inspire** your employees, customers, stakeholders, etc.
- This statement is a "best-case scenario" for the organization's future:

For 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.***

Sample Vision Statements (2019)

amazon

To be Earth's most customer-centric company

Google

To provide access to the world's information in one click

IKEA

To create a better everyday life for the many people

Instagram

Capture and share the world's moments

Microsoft

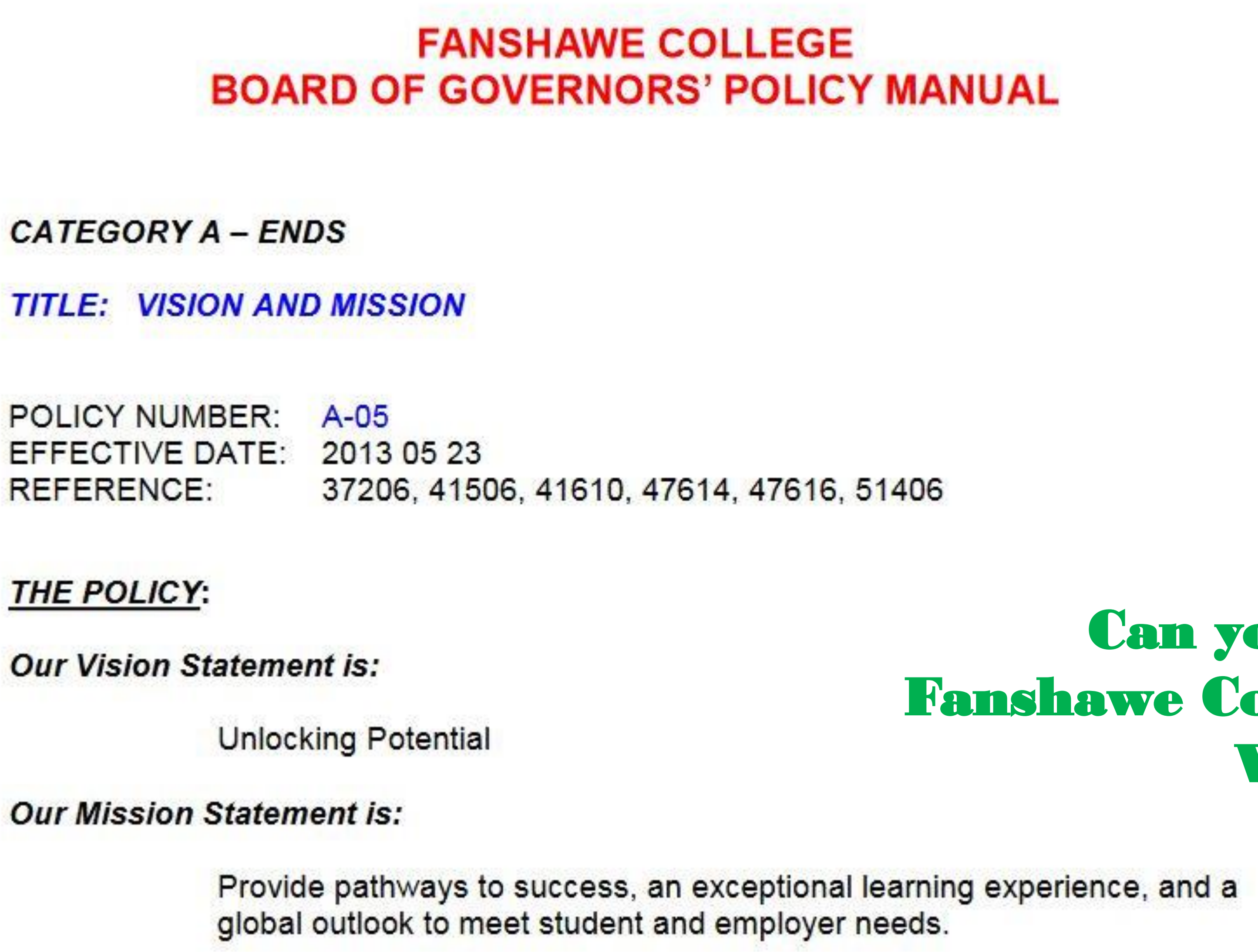
To empower every person and every organization on the planet to achieve more

NIKE

Bring inspiration and innovation to every athlete* in the world. *If you have a body, you are an athlete

Strategic Plan: Values Statement

- What does your company VALUE?
  - Example: integrity, honesty, passion, respect, environment, etc.
- Establishes a formal set of organizational **principles** and **qualities** to earn and keep the **trust** and **confidence**
- Gives companies a clear idea of who they are
- Makes organization’s conduct and performance standards clear
  - *Example: “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”*
- A declaration that announces a company’s top priorities and core beliefs



FANSHAWE COLLEGE
BOARD OF GOVERNORS' POLICY MANUAL

CATEGORY A – ENDS

TITLE: VISION AND MISSION

POLICY NUMBER: A-05
EFFECTIVE DATE: 2013 05 23
REFERENCE: 37206, 41506, 41610, 47614, 47616, 51406

***<u>THE POLICY</u>*:**

Our Vision Statement is:

Unlocking Potential

Our Mission Statement is:

Provide pathways to success, an exceptional learning experience, and a global outlook to meet student and employer needs.

Can you find Fanshawe College's Values?

Creating a Strategic Plan

- **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.**"
- Progresses from a general strategy (organization-level) to specific/operational Strategies (division-level) to tactical Planning (department/service-level)
  - These planning levels are discussed next…

Creating a Strategic Plan

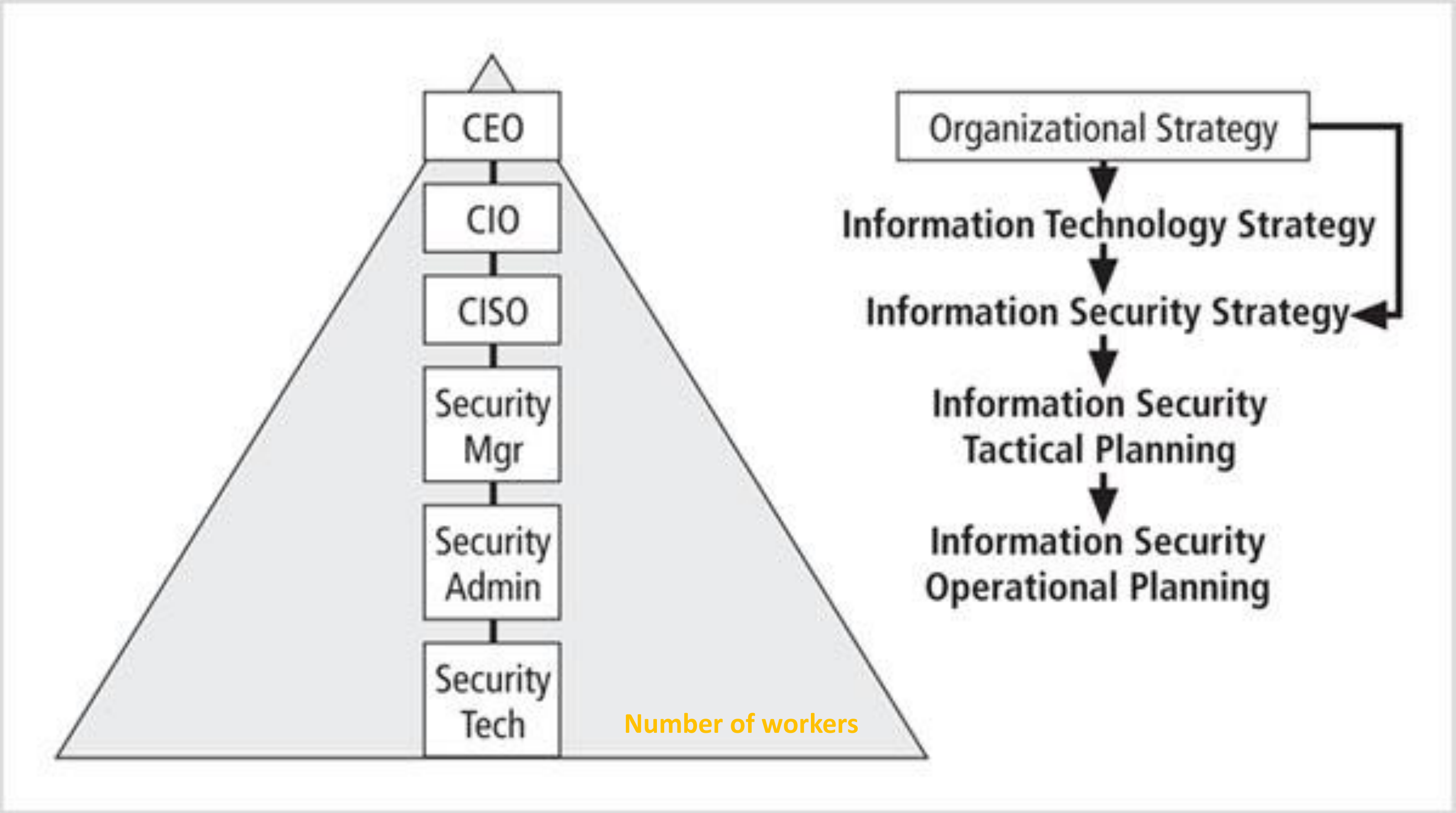

CEO
CIO
CISO
Security Mgr
Security Admin
Security Tech
Number of workers
Organizational Strategy
Information Technology Strategy
Information Security Strategy
Information Security Tactical Planning
Information Security Operational Planning

Figure 2-2011 Top-down Strategic Planning

Source: Course Technology/Cengage Learning

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
- In order to execute this **broad strategy** executives must define **individual managerial responsibilities**

- *For example, consider a sports team. The broad strategy (from the CEO) is to win the cup, but organization execs have to make decisions, then coaches and trainers, and eventually the players have to do the work on the field*.

Three Planning Levels

- Strategic Planning **(level 1)**
  - begins in the Board Room /Corner office
- Strategic goals are translated into tasks
- Objectives should be **(S.M.A.R.T.)**
  - **S**pecific,
  - **M**easurable,
  - **A**chievable, (also called "Attainable")
  - **R**easonably high (also called "Relevant")
  - **T**ime-bound
- Strategic planning then begins a transformation **from general objectives to specific objectives**

Three Planning Levels

- Tactical Planning **(level 2)**
  - –Often done at the departmental level
  - –Has a shorter focus (time-wise) than strategic planning
    - –Usually one to two years
  - –Breaks applicable strategic goals into a series of incremental objectives
  - –Department heads focus goals for **<u>their areas</u>** of responsibility

Three Planning Levels

- Operational Planning **(level 3)**
  - –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

How does a CISO make a Strategic Plan?

- Tell me some *possible* elements of a strategic plan?
  - Executive summary (less reading as rank increases ☺)
  - 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)

Creating a Strategic Plan

Tips for creating a strategic plan

- 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
  - Links strategic goals with performance
- Deploy a *draft high level plan* early, and **ask for input** from stakeholders in the organization
- Make the evolving plan **visible** (encourages ownership/buy-in)
- Make the process **invigorating for everyone**
- Be persistent (important to you = important to your team)
- Make the process **continuous and dynamic**
- **Be yourself and have some fun!! Planning is exciting!**

Governance

WHAT IS IT GOVERNANCE?

IT STRATEGY
BUSINESS STRATEGY

Information Security Governance

Who/What governs YOU?

(controls your decisions and actions)

Information Security Governance

- “the system by which an organization **directs and controls** IT security” (ISO 38500). ***Strategic planning responsibility.***

- Governance is a **management structure** that specifies the **accountability** framework and provides **oversight** to ensure that *risks are adequately mitigated*

- Ensures that security strategies are aligned with **business objectives** and consistent with **regulations**.

- Must be addressed at the highest levels of an organization's management team to be effective and offer a sustainable approach

- Importance of IT governance has grown in recent years. **Why?**

Information Security Governance

- NIST describes IT governance as "*the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility,* ***all in an effort to manage risk***".
- Information security governance includes
  - –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

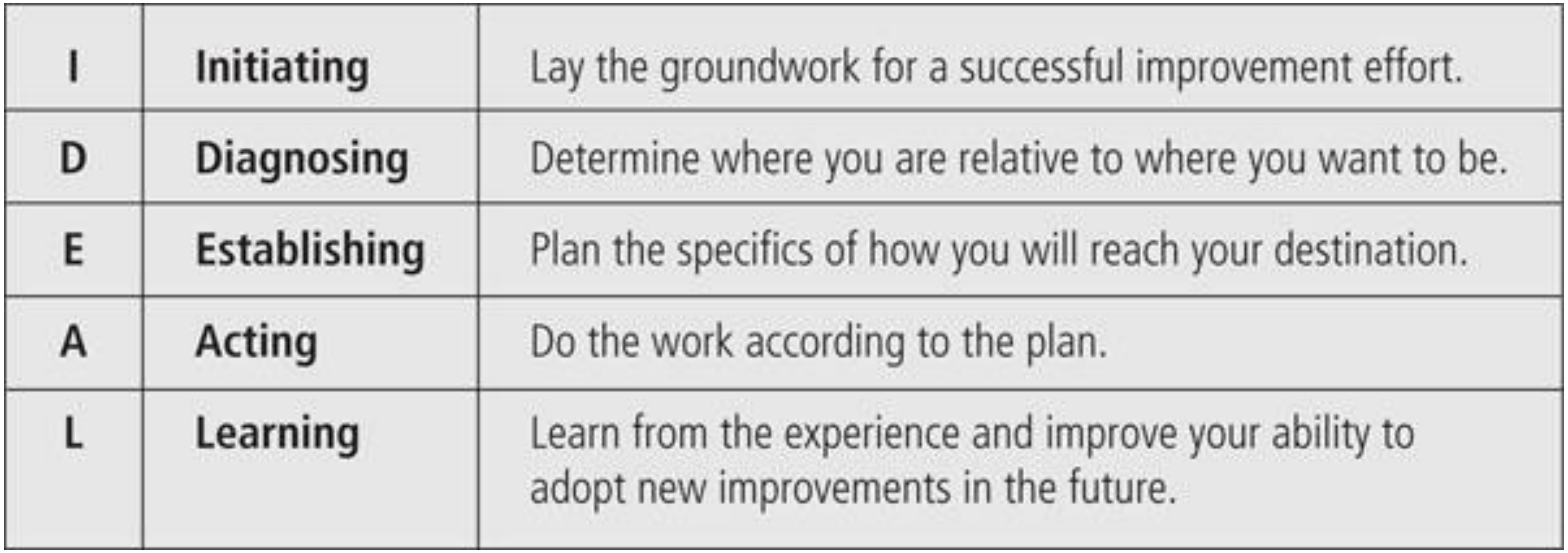
Desired Outcomes – “what success looks like?”

Five Outcomes of information security governance

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

Information Security Governance Framework

This is an organizational improvement model for implementing improvement actions



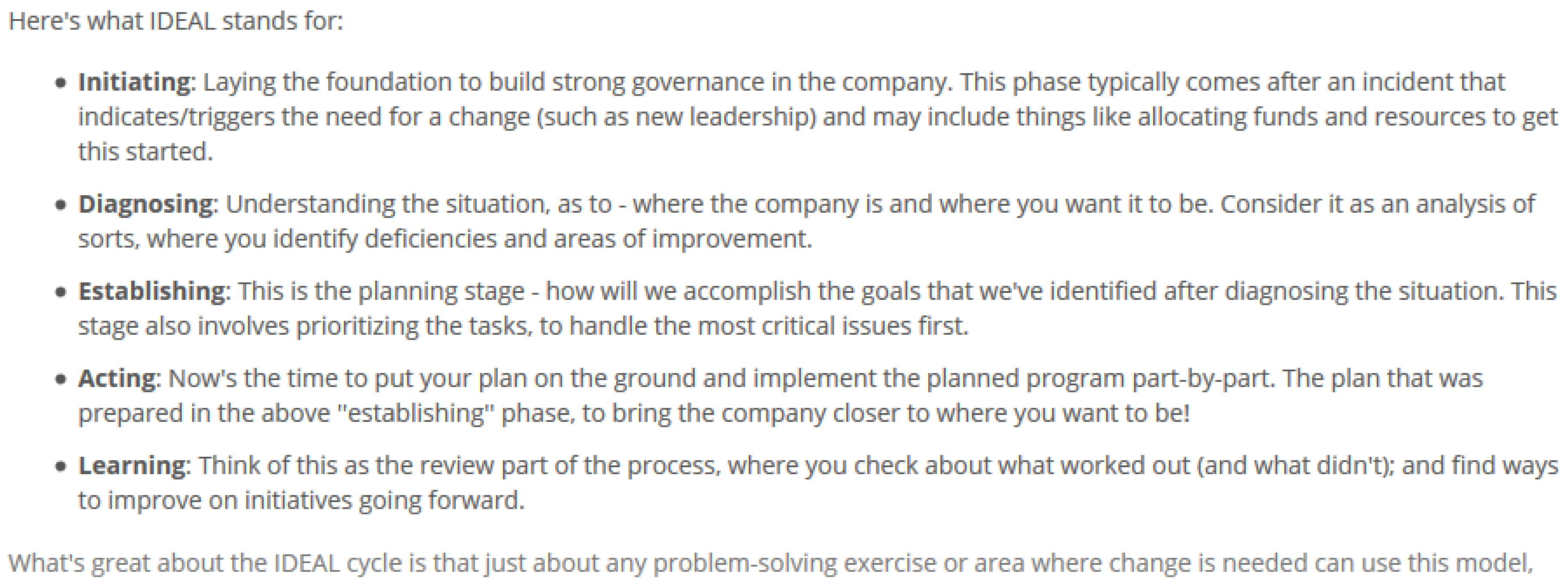
I	**Initiating**	Lay the groundwork for a successful improvement effort.
D	**Diagnosing**	Determine where you are relative to where you want to be.
E	**Establishing**	Plan the specifics of how you will reach your destination.
A	**Acting**	Do the work according to the plan.
L	**Learning**	Learn from the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

Figure 2-6 General Governance Framework

Source: IDEAL is a service mark of Carnegie Mellon University

Sounds similar to the ISO standard of PLAN, DO, CHECK, ACT, doesn't it?

NSCP’s IDEAL model



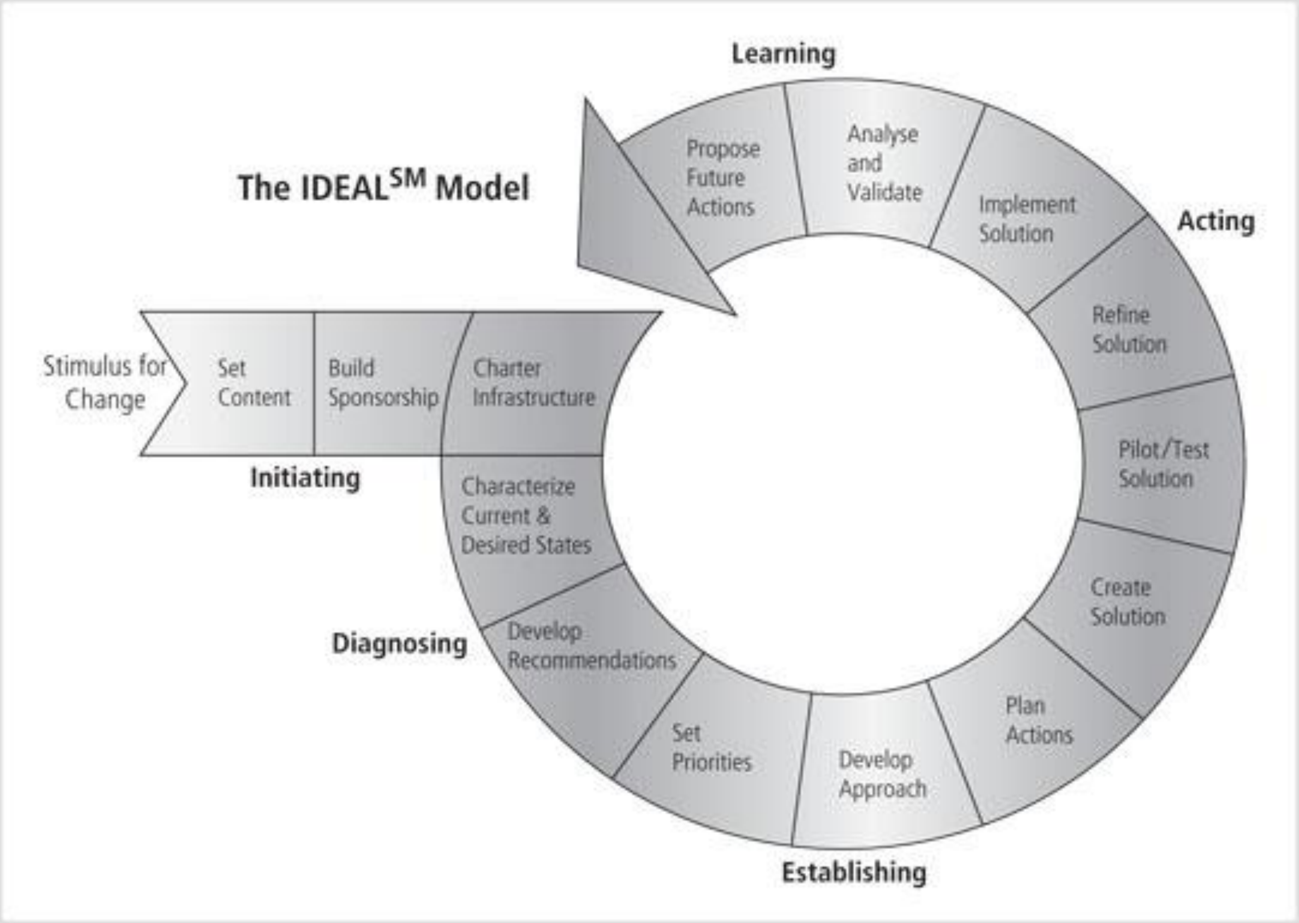
Here's what IDEAL stands for:

- **Initiating**: Laying the foundation to build strong governance in the company. This phase typically comes after an incident that indicates/triggers the need for a change (such as new leadership) and may include things like allocating funds and resources to get this started.
- **Diagnosing**: Understanding the situation, as to - where the company is and where you want it to be. Consider it as an analysis of sorts, where you identify deficiencies and areas of improvement.
- **Establishing**: This is the planning stage - how will we accomplish the goals that we've identified after diagnosing the situation. This stage also involves prioritizing the tasks, to handle the most critical issues first.
- **Acting**: Now's the time to put your plan on the ground and implement the planned program part-by-part. The plan that was prepared in the above "establishing" phase, to bring the company closer to where you want to be!
- **Learning**: Think of this as the review part of the process, where you check about what worked out (and what didn't); and find ways to improve on initiatives going forward.

What's great about the IDEAL cycle is that just about any problem-solving exercise or area where change is needed can use this model,

https://study.com/academy/lesson/ncsp-industry-framework-for-cybersecurity-governance.html

Information Security Governance Framework

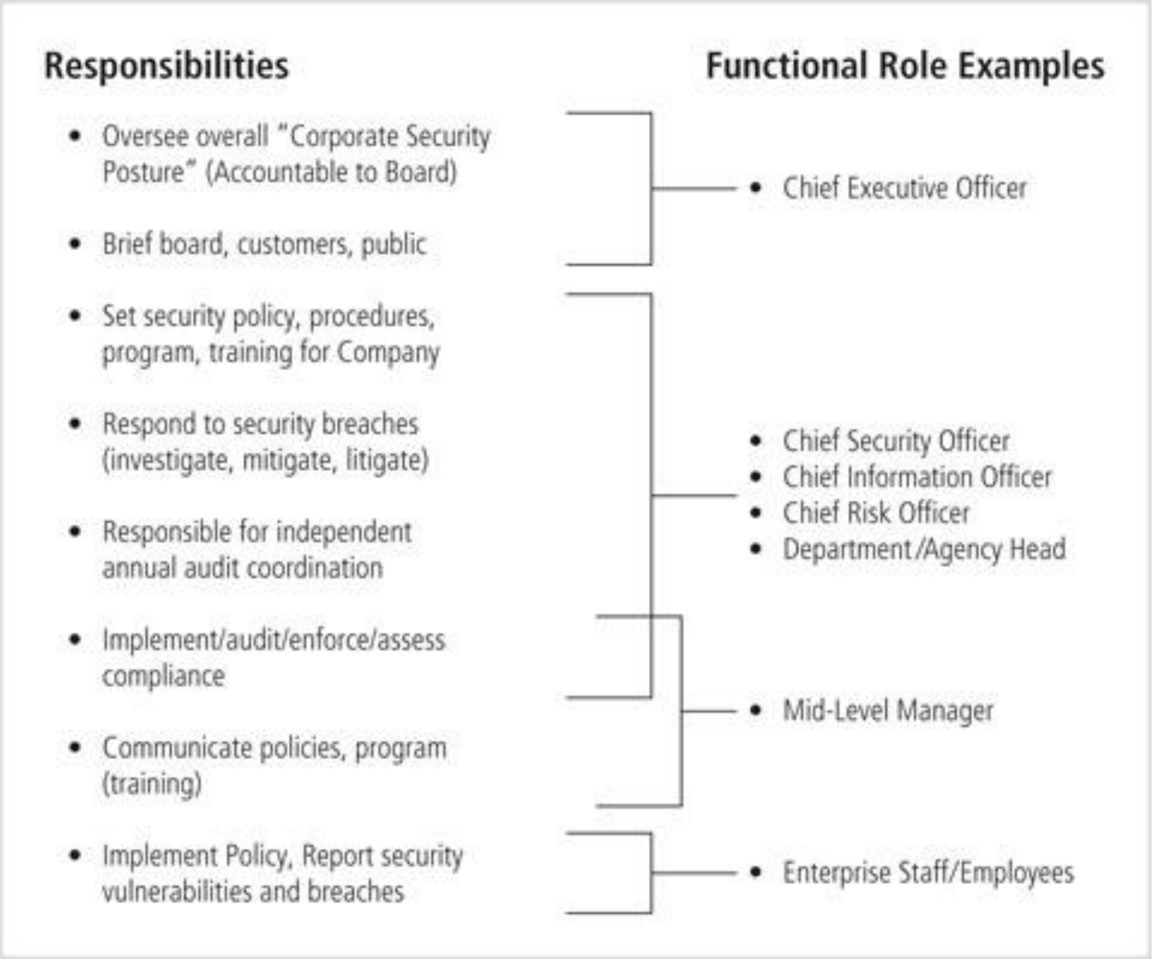


***TIP**: Use existing models, instead of creating your own from scratch!*

Figure 2-7 The IDEAL model governance framework

Source: IDEAL is a service mark of Carnegie Mellon University

Planning for Information Security Implementation



Responsibilities

- Oversee overall "Corporate Security Posture" (Accountable to Board)
- Brief board, customers, public
- Set security policy, procedures, program, training for Company
- Respond to security breaches (investigate, mitigate, litigate)
- Responsible for independent annual audit coordination
- Implement/audit/enforce/assess compliance
- Communicate policies, program (training)
- Implement Policy, Report security vulnerabilities and breaches

Functional Role Examples

- Chief Executive Officer
- Chief Security Officer
- Chief Information Officer
- Chief Risk Officer
- Department/Agency Head
- Mid-Level Manager
- Enterprise Staff/Employees

The IDEAL framework defines/governs the ***responsibilities of each functional role***

Figure 2-8 Information security governance responsibilities

Source: *Information Security Governance: A Call to Action*

Planning For Information Security Implementation

- Roles of the CIO and CISO/CSO
  - 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
  - CIO charges the CISO and other department heads with creating and adopting plans that are **consistent with** and supportive of the entire **organizational strategy**

Planning For Information Security Implementation

- CISO Job Description *(a sample)*
  - –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

NOTE the emphasis on BUSINESS (not TECHNICAL) skills?

Planning For Information Security Implementation

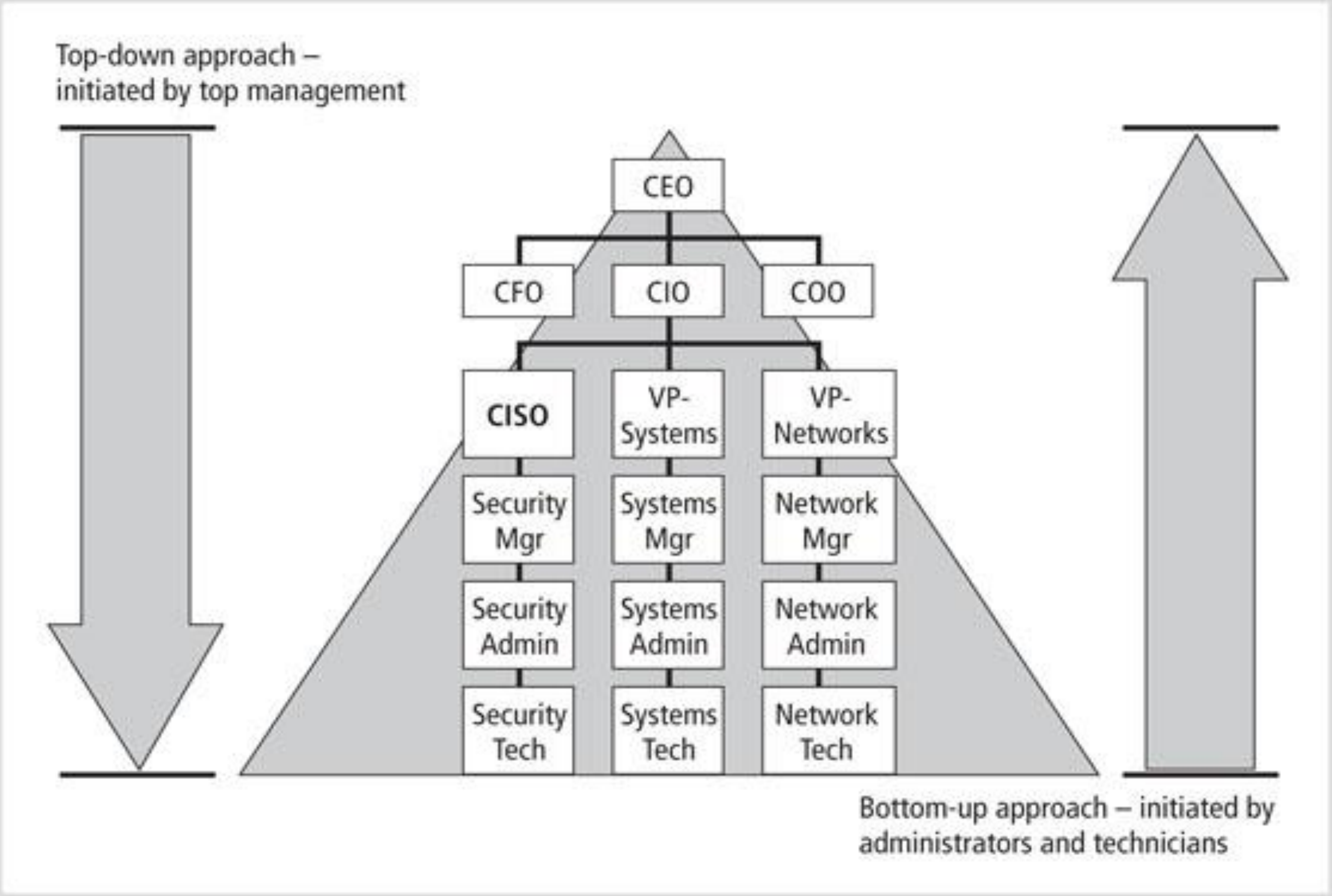


Figure 2-9 Approaches to security implementation

Source*: Course Technology/Cengage learning*

Governance Frameworks

- ITIL
- COBIT
- ISO standards

Data Governance

- Protects against cyberattacks and security breaches
- Reduces data management costs
- Increases ROI of your data analytics
- Lightens the IT team's data management load
- Allows for better decision making and communication
- Makes compliance standards easier to maintain

VARONIS

Often compared to each other: https://www.simplilearn.com/cobit-vs-itil-article

And now on to…

SecSDLC (or SSDLC)

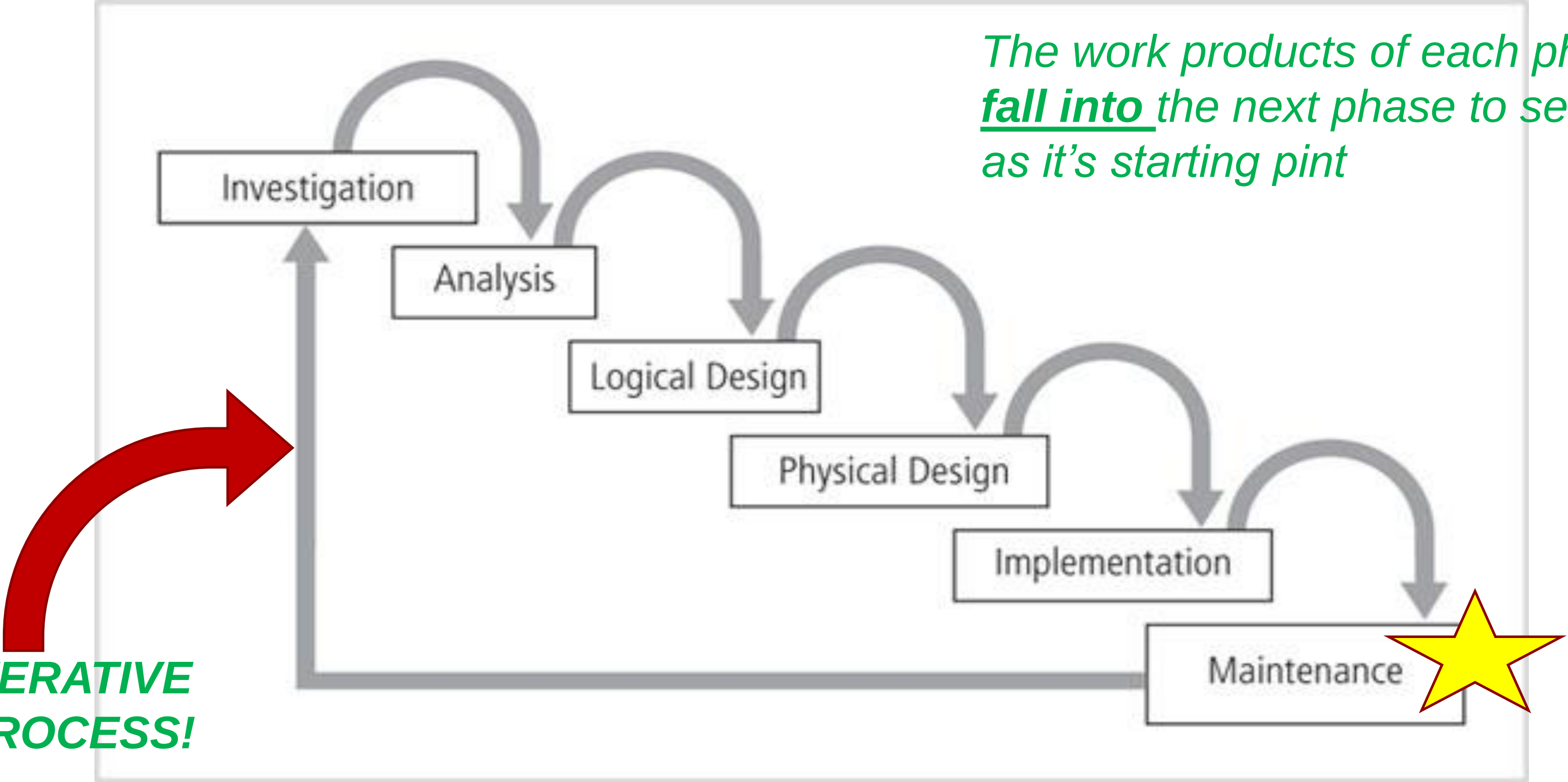
Software Development Life Cycle (SDLC)

- An SDLC is a conceptual model for describing the phases (stages) in an IS/IT development project.
- It is a ***methodology*** (a formal approach to solving a problem based on a structured ***sequence of procedures***) for the design and implementation system in an organization
- If a methodology works, keep using it!
- SDLC-based projects may be initiated by events (event-driven) or planned (plan-driven) as part of a strategy
- At the end of *each phase*, a **structured review** (“reality check”) occurs to determine if the project should be continued, discontinued, outsourced, or postponed until additional expertise is acquired

Security Systems Development Life Cycle

- SecSDLC methodology is similar to SoftwareDLC
  - A variation of the SDLC methodology, it is used to create “a comprehensive **security posture**”
  - The SecSDLC process involves the **identification of specific threats**, the **risks** that they represent, and the subsequent design and implementation of specific **controls** to counter those threats and manage the risk
  - The process turns infosec into a **coherent program** rather than a **series of responses** to individual threats and attacks

SecSDLC – a “waterfall” model



The work products of each phase ***<u>fall into</u>*** *the next phase to serve as it’s starting pint*

ITERATIVE PROCESS!

Figure 2-10 Phases of the SecSDLC

Source*: Course Technology/Cengage learning*

Active Learning Exercise

- Consider each of the 6 phases of SecSDLC (discussed in the next 18 slides)
- Choose the TWO phases that you feel are the most important to an organization.
- Justify your selection. Why these two and not the other 4?

- How does security system development life cycle reduce security risks of an organization?

1. Investigation Phase

1. Investigation Phase in the SecSDLC

- –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 Study/Analysis and Needs Assessment
  - Hypothetical exercise
  - Determines whether the organization has the resources and commitment to conduct a successful security analysis and design

2. Analysis Phase

2. Analysis Phase 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

2. Analysis Phase

- Additional SecSDLC definitions:
  - An attack
    - –A 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 assets
  - An exploit
    - –A technique or mechanism used to compromise a system
    - –A threat agent will exploit a vulnerability in the system
  - A vulnerability
    - –An identified weakness of a controlled system in which necessary controls that are not present or are no longer effective
    - –“plug the hole”

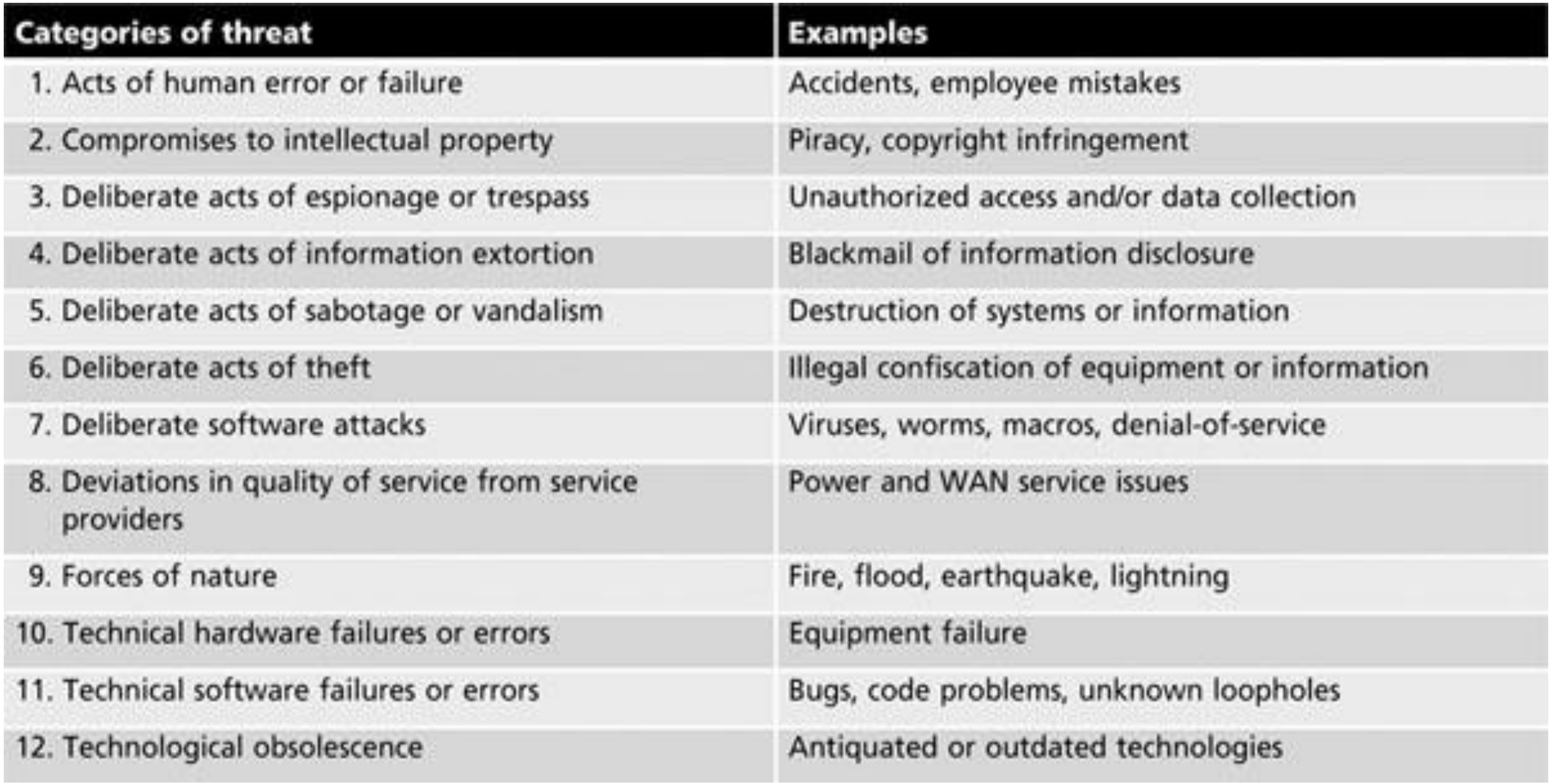
2. Analysis Phase

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

- Prioritize the risk posed by each category of threat. Most serious?
  - ✓ Don’t ignore low-level risks!

- Identify and assess the value of your information asset
  - Assign a comparative risk rating or score to each specific information asset

2. Analysis Phase



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

Table 2-1 Threats to Information Security

Source: Course Technology/Cengage Learning (adapted from Whitman, 2002011)

3. Design Phase (Logical)

3. Logical Design Phases in the SecSDLC

- –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

- Security **models** may be used to guide the design process
  - –Models provide frameworks for ensuring that all areas of security are addressed. *Frameworks help us make sure we don't miss anything!*
  - –Organizations can adopt or adapt/customize a framework to meet their own information security needs
  - –Documentation! Write things down (like goals). Make lists.

3. Design Phase (Logical)

Design controls and safeguards

- –Used to protect information from attacks by threats
- –Three categories of controls: managerial, operational and technical

- **Managerial controls** are in place to direct management
  - –Address the design and implementation of the security planning process, security program management, risk management, and security control reviews
- **Operational controls** cover lower-level (planning and personnel) at the ground level
  - –Disaster recovery, incident response planning, personnel security, physical security, protection of production inputs and outputs

3. Design Phase (Logical)

- **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
  - –“Set it and forget it”?
- Contingency planning / BCM
  - Prepare, react and recover from circumstances that threaten the organization
  - Types of contingency planning
    - –Business continuity planning (BCP)
    - –Disaster recovery planning (DRP)
    - –Incident response planning (IRP)

4. Design Phase (Physical)

4. Physical security Phase in the SecSDLC

- –Design, implementation, and maintenance of controls (safeguards & countermeasures) that protect the physical resources of an organization

- Physical resources include
  - –People
  - –Hardware
  - –Supporting information system elements

4. Design Phase (Physical)

- A critical design element of the information security program is the **enforcement** of the design **through** information security **policy**
  - Consequences act as deterrent to non-compliance
- Management must define three types of security policy
  - ➢Enterprise information security policies
    - ❖Top level – applies to everyone and everything
    - ❖Keep it short – maybe 1 page long. Lower-level policies are more specific
  - ➢Issue-specific security policies
    - ❖Ex. Access Control, Cryptography
  - ➢Systems-specific security policies
    - ❖Management of a firewall, hardening an operating system. Very detailed

“Law governs nations, Policy governs businesses.”

4. Design Phase (Physical)

- Security Policy at all levels must be communicated as a control. Why do we have rules? *To safeguard our assets and implement countermeasures when required.*

Education and Training are KEY to controls

✓How can they behave correctly if no one shows them how?

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

5. Implementation Phase – Let's Do it!

5. Implementation Phase 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

5. Implementation Phase – Choose your team

- Members of the Implementation/development team
  - Champion
  - Team leader (herding cats? The people problem)
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

Do you like working as part of a team?

5. Implementation Phase

- 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 info security across every role in IT
  - –Integrate solid information security concepts into the personnel management practices of the organization
  - –is InfoSec the same as ITSec?
    - –Different reporting structure
    - –Different role – policies/audits/maintenance, vs. passwords/firewall/VPN/AAA

5. Implementation Phase

- Information security professionals
  - Chief information officer (CIO)
  - Chief information security officer (CISO)
  - Security managers
  - Security technicians
  - Data owners/creators vs Data Custodians vs Data Users
    - Confidentiality Classification: Who determines the confidentiality level?
      - Remember that data confidentiality classification may change over time (private > public)
- Professional certifications
  - CISSP (Certified Information Systems Security Professional)
  - SSCP (systems Security Certified Practitioner)
  - GIAC (Global Information Assurance Certification) (*cybersecurity*)
  - Security + (CompTIA)
  - CISM (Certified Information Security Manager)

***Should the highest rank (ex. CIO) hold the most certifications?*

6. Maintenance Phase

6. Maintenance Phase in the SecSDLC

- –Includes change when needed
- –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

6. Maintenance Phase

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

6. Maintenance Phase

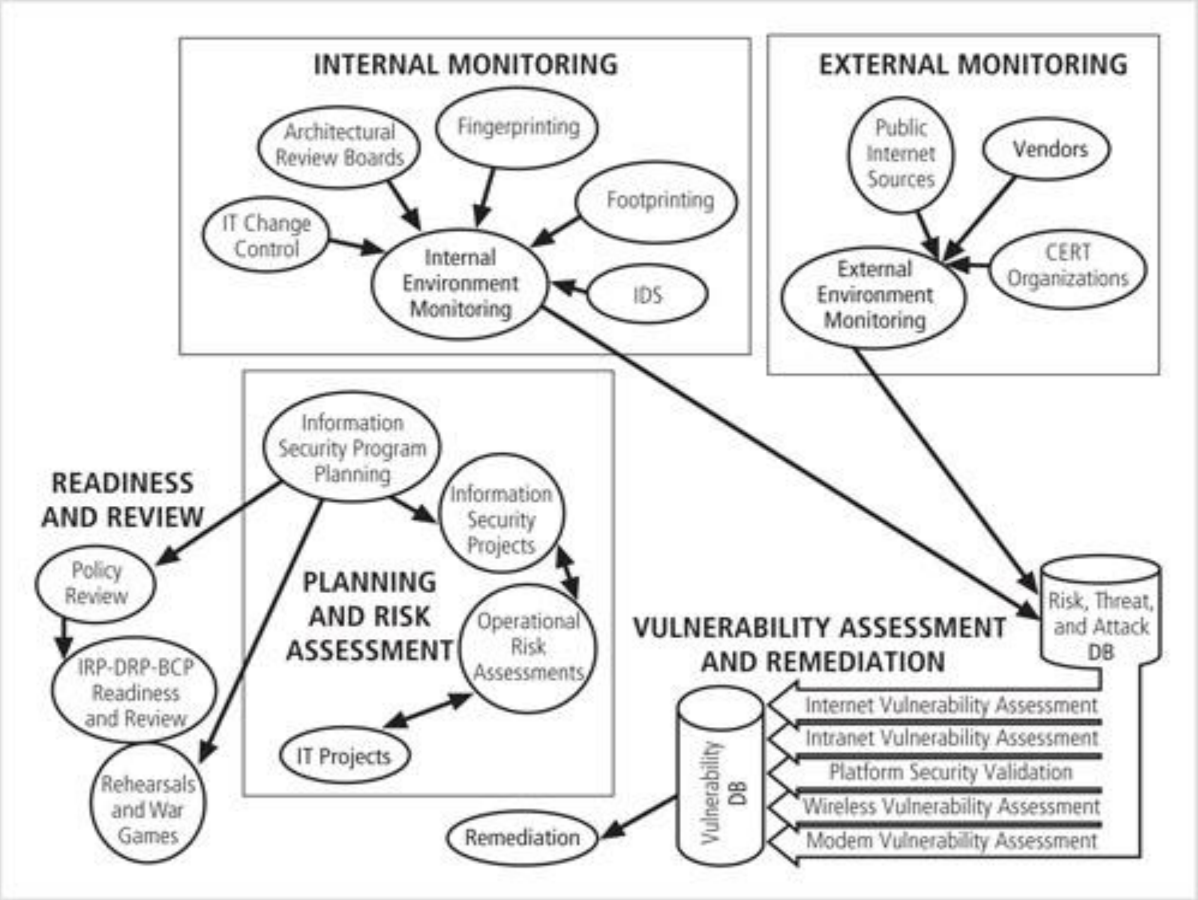

INTERNAL MONITORING
Architectural Review Boards
Fingerprinting
Footprinting
IT Change Control
Internal Environment Monitoring
IDS
EXTERNAL MONITORING
Public Internet Sources
Vendors
CERT Organizations
External Environment Monitoring
READINESS AND REVIEW
Policy Review
IRP-DRP-BCP Readiness and Review
Rehearsals and War Games
Information Security Program Planning
Information Security Projects
PLANNING AND RISK ASSESSMENT
Operational Risk Assessments
IT Projects
Risk, Threat, and Attack DB
VULNERABILITY ASSESSMENT AND REMEDIATION
Internet Vulnerability Assessment
Intranet Vulnerability Assessment
Platform Security Validation
Wireless Vulnerability Assessment
Modem Vulnerability Assessment
Vulnerability DB
Remediation

Figure 2-11 Maintenance model

Source: *Course Technology/Cengage learning*

- Security program management
  - A formal management standard can provide some insight into the processes and procedures needed
  - Examples include the BS7799 / ISO17799 / ISO27xxx model or the NIST models (800-series) described earlier

Discussion Forum Ideas for This Week

1. Your personal Learning Debrief is definitely still an option if you haven’t done that yet

2. Talk about gaming and **gamification** in cybersecurity. Is it helpful to use games to recruit/develop talent? How and why?
   - Is it wrong to assume young people would prefer to “game”?
   - What are your fav games? Could that ***style*** be used to develop?

3. Regarding the discussion on the IT skills gap, write about your personal journey into employment in this field. What have you learned in your research? where have you applied? what have you learned? What/which skills are in demand? Which certifications? What are your prospects for your “dream job”?

Homework and Reminders

- Assignment 2 is due today (March 10th)

- Assignment 3 will be released next week and (will be due at the end of week 11)

- Test week 10 is worth 15%.
  - What is your PLAN to succeed on the test?
  - Study in groups! ☺
  - Which leads us to the discussion forum idea for this week….

Thank you for being here!

Any questions?

FANSHAWE