INFO 6027

Information Security Planning

Week 1 - Introduction

FANSHAWE

A “wake-up” riddle…

It has keys but no locks. It has space, but no room. You can enter, but can’t go inside. What is it?

Rosie Nanji

- Professor, School of IT
- Room G3001
- 519-452-4430 x4899
- r_nanji@fanshaweonline.ca

- **See short bio on FOL Discussion Forum ☺**

Agenda

Today's Lesson

- **Part 1: Introduction to the course**
  - Orientation highlights
  - Housekeeping / Routine
  - Course Overview, Syllabus and Expectations
- **Part 2: Lecture/Discussion**
  - What is Information Security Management?
  - ISM vs general business management
  - What are some key characteristics of information security, leadership, managers
  - Roles and Responsibilities
  - Reminders for next week

Orientation Highlights
Winter 2023

FANSHAWE

Welcome to Fall 2022 Term!

- Did you attend orientation Tuesday Jan 03?
  - Led by our program coordinator, Mr. Clive Wright
  - Any questions from that session? (you can also email and/or post in discussion forum)
  - A special welcome to **any first timers** in the class !
- A few **highlights from orientation**:
  - WELCOME! We are very happy you are here ☺
  - Your instructors **want to see you succeed**
  - Please don't cheat – consequences are severe
    - **What constitutes cheating?**
  - You must submit assignments on time. Late assignments are not accepted.
  - Despite COVID, there are still **a lot** of resources and services available to you
  - Fanshawe Online (FOL) is your ultimate resource for this course/program
  - Textbooks are expensive, but **there are options**

Other Highlights from Orientation

- Clive Wright, ISM/NSA Coordinator also talked about:
  - Laptop specs
  - Booklists available online
  - If you are an NSA grad, you might PLAR the THREE common courses
  - Allow approx. **2 business days** for email responses from professors
  - We do not allow re-writes for missed assignments and tests
  - Use every resource available to you. **What are some resources?**
  - **Time management** is critical (part-time jobs? Family? Time zones? Challenges working remotely?)

Job hunting?

- How many of you intend to work (either full or part-time) while you are students?
  - What is your **PLAN** to address the challenges with time management?
  - Have you booked off your **exam week (April 17-12)?** You should!
  - Prioritize SCHOOL over work. This includes study time as well (8 hours per day).
- You can also use Fanshawe's Career Services office for employment help
  - Ex. Interview practice, resume and cover letter help, search job postings, etc.

More Orientation Notes…

- ***Don't wait*** to get help if you are struggling. **Ignoring the problem will not solve it**
- Peer tutors are paid by the college to help you. *Please use them*. Online chat.
- You need a GPA of 2.0 or higher to graduate
- This is a 14-week term (late start).
- Mid-term grade (week 6) is either an S or a U.
- DO NOT pull "all-nighters". Research shows these actually lower your academic performance
- Written notes help commit ideas to memory. Consider a digital flash card deck!

Student Success

- Please prepare for the lectures BEFORE you attend (or listen to) them
  - **How to prepare?**
  - Do not “binge watch” the lessons. Works for Netflix – not for learning!
- Taking notes (and asking questions) is essential to your success
- Prepare properly for tests – include your laptop, power supply, cables,
- Do **all** the homework – *even the recommended work*.
- Do not miss tests or assignments

Other highlights from Orientation

- Michelle Prestwich at mprestwich@fanshawec.ca– Student Success Advisor
  - Your resource for questions about your success, options, decisions
  - Connect via email, not phone
  - Attendance is critical to success
  - Strongly urge you to use the **peer tutors** and peer mentoring sessions (both are FREE!!)
  - Your success depends on your ability to balance/manage your time
    - Too much books = burnout
    - Too much beer = flunk out
  - If you are an **international** student, practice speaking English all the time – especially to other international students
  - Budget an hour of homework for every hour of class. TREAT IT LIKE A FULL TIME JOB
    - How many hours in a full-time job?

Let’s talk about the INFO 6027 course

FANSHAWE

The Routine

- At the start and end of each class I'll take some time to remind you of upcoming tests/assignments (aka my "Housekeeping" slide)
- Synchronous classes will start with a **virtual "check in"** to see if there are any questions stemming from last week, and generally see how you are doing/feeling with your course load.
- We will also explore **current events**, news items, and other resources relating to Security Planning and ISM in general.
- ISM is a ***student-centered*** program. *Your learning is paramount. Own* your learning!
- Then we will proceed with an interactive lesson
  - **Come prepared for class**
  - **Be prepared to work in breakout groups during tutorial**
- Will conclude each lesson with an invitation for **questions** and reminders for the coming weeks

Current Events: What is happening in (your) world?

- Let's look at: https://threatpost.com/

Fanshawe Online

- Fanshawe Online **INFO-6027 Security Planning (W23)** is the course name on FOL.
  - Stay tuned to the "**Announcements**" section. Check it often!
  - Sections include Content, Communications, Evaluations, Media Tools, etc

Classroom Conduct

- Testing
  - Written quizzes and exams use the **Respondus Lockdown Browser (RLDB)**
  - Recommend you find a quiet place to write tests (not always easy!)
  - Hard-wired ethernet access is preferable to wireless (RLDB hates signal drops)
  - Working, **tested**, fully powered laptop
    - **Take the test quiz** to make sure you have RLDB correctly installed and configured.

**Time lost due to PC problems is not recoverable

Student Success

- This is a “Lecture style” class, which means that *it is instructor-led*, but **I will not lecture to you**.
- Lots of interactive exercises and (hopefully) discussions during class time
- I suggest you take notes during the lecture, as *not all test questions come from the PowerPoint slides and textbook!*
- Slides are a HANDOUT that highlights key points, but they do not cover all you need to know.
- Not all concepts are fully explained on the slides. You need to do the exercises and listen to/participate in tutorials.
- Everything in the lessons / resources / discussion is **testable material**.
- **Ask questions** if you don’t understand something – **you likely won’t be the only person**.
- Don’t try to memorize! Memory alone will not suffice. **Understanding** and **application** are key!!
- Do not underestimate the work required for this course/program

Student Success

- Show respect for your professor and your peers
  - **Be active and participate** in online class discussions
  - **HELP EACH OTHER**. Create your own study groups (or use the discussion forum). Some of you may solve problems faster than your peers – share your success by showing them how!
- **Prepare properly** for lectures and tests
- Do **all** the required ***and recommended*** work
- Do not miss tests

The Course Outline

FANSHAWE

Course Outline

- Learning Outcomes
  - What you **will be able** to demonstrate once the course is completed.
  - Questions on tests will reflect your attainment of these objectives

- Course Plan
  - Detailed list of what you should expect to be taught each week
  - How to prepare for class
  - Test and assignment due dates

Course Design

- 3 hours/week of class time (but budget at least 2hrs/week homework)
  - Videos, recordings of tutorials, whole class discussions, scenarios, etc.
  - Preparation for next class, reading the chapters, study ahead!
- Class time will consist of:
  - 100% - Discussions, Lecture, and Review

- **Note**: We will take **frequent breaks** during the lesson/lecture/tutorial. Breaks help us all **to maintain our focus and concentration**.

INFO 6027 – Learning Outcomes

This course is designed to help you meet specific learning outcomes.

- There are **11 course learning outcomes**.
- EVERYTHING we do in this course is designed to help you meet those outcomes
  - If you are **not clear** as to how a task/content relates to these outcomes, **please ask!**
    - **#ownyourlearning**
- Note the active tense of the outcomes – they are also future-focused. What you will learn, know, understand, apply, develop, identify, create, describe, explain, etc.

INFO 6027 – Information Security Planning

Some of the topics we will cover in this course:

- What is an ISMS?
- Threats, Risks, Assets, Vulnerabilities
- BIA, BCP, DRP, DAP, Risk Assessments,
- ISO Standards, plans and procedures, popular models
- Governance and Incident Management
- Types of security policies, creation, purpose, examples
- Roles and responsibilities within an organization
- HR Security and training the workforce (ex. SETA)
- Relevant legislation and Ethical considerations

Course Overview

- Implementing an Information Security Management System (ISMS)
- Most common InfoSec Methodologies
- BCM – Business Continuity Management
  - Definition, Need, Best Practices, Tools
  - Business Impact Analysis - InfoSec
  - Contingency Planning - InfoSec
- Planning, Planning, & more planning for avoiding bad outcomes in:
  - Corporate Politics, Finance, Projects, Security Management, Disasters, etc
- Policy design, delivery, education, upkeep
- Privacy and Security Law, Ethics, Procedures
- **This is the "macro" class**. Foundational knowledge of InfoSec management. We look through the lens of overviews and broad concepts. Occasional deep dive.

How will you be evaluated in this course?

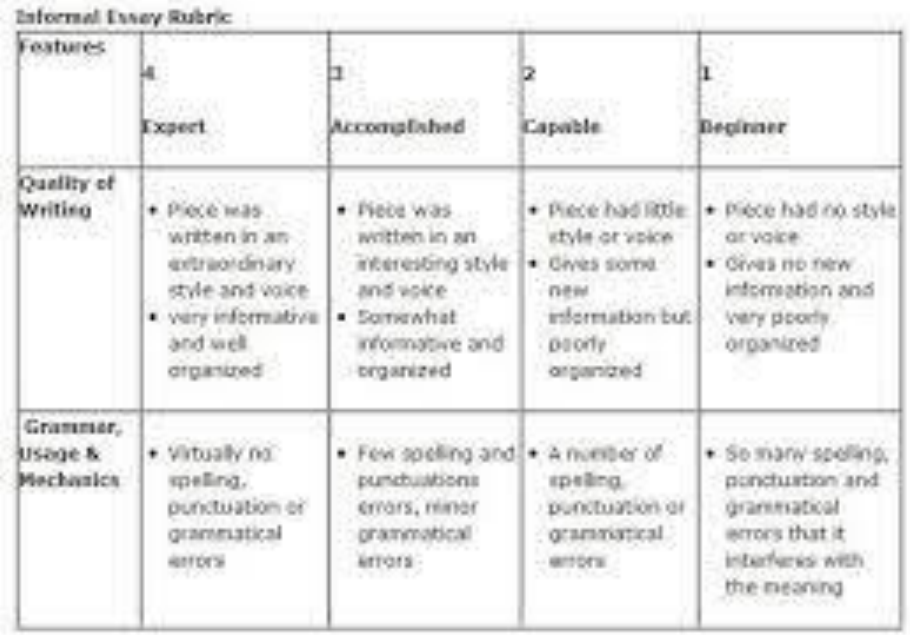
Testing! There are THREE tests in this course

- All quizzes and exams use the **Respondus Lockdown Browser**
- ***Tests are NOT open book***
- Recommend you use wired ethernet and a plugged-in power supply (Respondus does not like power/network blips!)
- Working **AND tested** PC or laptop (use the mock quiz to test!)
- Expect an **average** time of **30-60 seconds per question**
- Short answer, long answer, M/C, T/F, FIB, Matching,
- **All tests are manually graded by me.**
- Testable material includes anything discussed “in class” (both verbally and on the slides), in the textbook, any articles or resources I share, and in the labs.

Test time lost due to PC or Respondus problems is not recoverable.

Course Outline

- Assessments
  - READ THE RUBRICS!
  - Three written assignments (10% each)
  - 2-unit tests (15% each)
  - Final exam (40%)



Informal Essay Rubric

Features	4 Expert	3 Accomplished	2 Capable	1 Beginner
Quality of Writing	• Piece was written in an extraordinary style and voice • very informative and well organized	• Piece was written in an interesting style and voice • Somewhat informative and organized	• Piece had little style or voice • Gives some new information but poorly organized	• Piece had no style or voice • Gives no new information and very poorly organized
Grammar, Usage & Mechanics	• Virtually no spelling, punctuation or grammatical errors	• Few spelling and punctuations errors, minor grammatical errors	• A number of spelling, punctuation or grammatical errors	• So many spelling, punctuation and grammatical errors that it interferes with the meaning

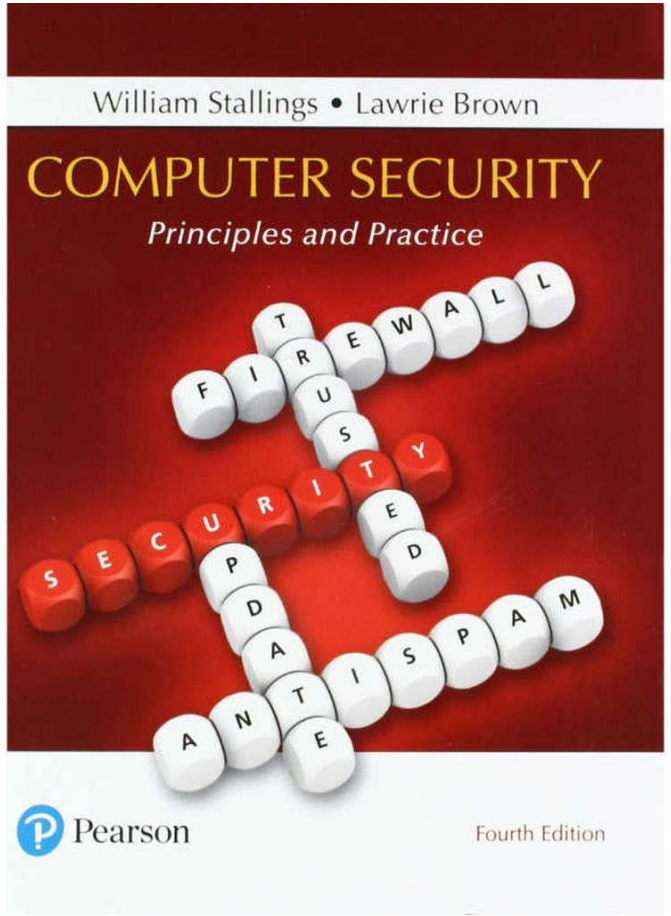
- Textbook for this class is the Stallings and Brown book "Computer Security Principles and Practice" (4th Ed. 2018), **but you should also:**
  - use online resources
  - Watch relevant videos
  - Find case studies and apply what you are learning to those cases

Grading

- **Rubrics** are used for all written assignments.
  - What is a rubric?
  - Writing skills are graded, references are required, formatting is graded
  - Content, flow, grammar/spelling
  - Submit via **Evaluation > Submission** in FOL by the deadline
  - **You WILL receive detailed, specific, and constructive feedback from me**

Criteria	Level 4 5 points	Level 3 4 points
Content: Clarity and Depth	All questions are answered completely. Responses demonstrate a depth of analysis and critical thinking, materials, and ideas from the course, are ingrained in each response. Explanations and justification for decisions are provided	Most questions are answered completely. Most responses demonstrate a depth of analysis and critical thinking, materials, and ideas from the course are ingrained in each response. Explanations and justification for decisions are provided in most cases
Organization and Readability	No spelling, grammar, or sentence structure issues. Ideas flow logically from one to the next, making the paper very easy to read. No issues with sentence structure. All ideas are discussed in sentence form (Point form is not used in the document except when showing a list).	Very few spelling, grammar, or sentence structure issues. Most ideas flow logically from one to the next, making the paper relatively easy to read. Less than 3 issues with sentence structure. Most ideas are discussed in sentence form (Point form is used sparingly in the document).
References, Formatting and APA Compliance	Paper is fully compliant with APA 6th Ed. standards other	Paper is mostly compliant with APA 6th Ed. standards

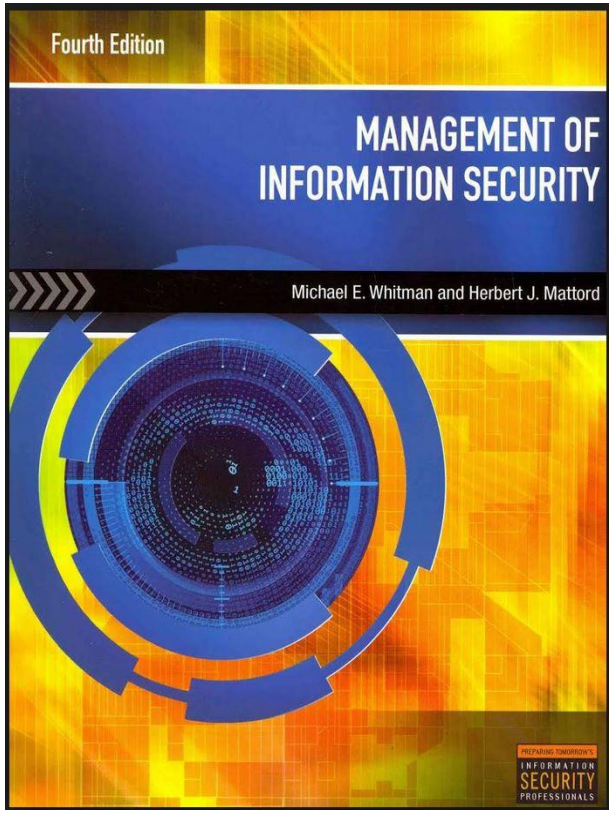
Required Text



- Computer Security – Principles & Practice
- 4th Edition (2018)
  - William Stallings and Lawrie Brown
  - Pearson - Prentice Hall
  - ISBN:978-0-13-377392-7
- *Previous editions are better than nothing!*

Recommended Text and Other Resources

- Recommended Reading List (under Resources)
  - Selections from Stallings textbook
    - Online Chapters 25 & 26 – Premium Content with Textbook Content Code
  - Microsoft Security Publications
  - ISO standards
  - Other documents as provided or recommended in FOL and lectures
  - Experiences – Both yours and mine
  - Security news items (articles and recent events)
  - Exercises (ALE's)
  - Readings - Management of Information Security
    - By Whitman and Mattord
  - Mock tests, review questions, chapter summaries, key terms, etc.



Course Expectations

- Missed Assignments and Tests
  - Students are **not entitled** to complete missed tests
  - In case of a significant event supported by documentation AND professor's approval AND prior notification, a missed test *may* be completed
- Re-writes & extra grade items
  - Students will **not be permitted** to rewrite tests
  - Students will **not be entitled** to extra work or assignments in order to raise a grade

- **Assignments are written.** Writing skills are critical in information security and in business. You will be evaluated on your RESEARCH and WRITING skills
  - **Use an editor** (if you are not comfortable with writing in English, for example)
  - **Collaboration is encouraged**, but DO NOT COPY. Plagiarism is severely penalized.

Assignments

- Hand in ALL assignments on time. I will not accept late assignments.
- Put the assignment name and your last name in the file name
  - (ex. Robertson-Assign1.doc). I prefer you use Microsoft Word for written assignments.
- Assignments must follow APA-style formatting and referencing
- All assignments must be submitted via FOL in the correct submission box
  - **Assignments submitted in any other method (including email) will not be accepted**
  - Assignments submitted using the wrong submission box will not be graded.
  - Submission box is open until the noted time, for example 11:59pm.
  - You must *complete the submission process* before this time.
  - Assignments **must have references** - Failure to do this may result in an academic offense

Learn to love APA ☺

- APA is one method of formatting your paper and your references
- ALL of your written work should comply with APA standards
  - This is in the rubric!
  - Discussion forum exempt from APA, but you must still reference work you use
  - Always have a title page and a References page
  - APA format includes margins, section headings, font, and more
- See the Fanshawe College Library website for help with APA
- The reason you are required to use APA on your written work is because professional writing is a critical skill for employment.
- It also helps you avoid an academic offence
- Great resource for you: https://owl.purdue.edu/owl/purdue_owl.html

Dates to remember

HIGHLIGHTS:

- **Assignment 1**: Due Week 3
- **Test 1** – 15%: Due Week 5
- **Assignment 2**: Due Week 8
- **Test 2** – 15%: Due Week 10
- **Assignment 3:** Due Week 12
- **Final Exam**: Due Week 14

Recordings

- Classes will be **synchronous** (but recorded for asynchronous viewing)
- **Please attend all lectures**
  - Participation is critical to learning.
- All times are EST (Eastern standard time)
- ALL lectures will be recorded, so if you have to miss a class or are in a distant time zone, you can still remain current.
- Doctor's notes are **not** required for missed tutorials

Part 2: What is Security Planning?

FANSHAWE

Week 1 – Agenda

- List and discuss the key characteristics of information security
  - Definition, CIA triad, Security Models, Threats, Terms, Management Styles,
- Describe the importance of the **manager's role** in securing an organization's use of information technology and explain who is responsible for protecting an organization's information assets
- Discuss the key characteristics of **leadership** and **management**
- Differentiate information security management (ISM) from general business management

Learning the Language:
Key Terms, Concepts, and Models

FANSHAWE

Introduction to some key terms

- What is a **plan**? How did you plan to get here? What is your academic plan? Career plan? Family plan? **PLANS are driven by GOALS**
- *"if you fail to plan, then you plan to fail"*
- What is ICT?
  - Enables the storage and transportation of information from one business unit to another
  - IT and *voice* systems can (and will) break down. **Tech Happens!**
- The concept of **computer security** has been replaced by the concept of **information security**
  - Why? Because InfoSec covers a broader range of issues from protection of **data** to protection of human resources
- Information security is the responsibility of *every employee,* including *managers*.

Key Terms (continued)

- Security requires investment! (Support and budget $$ can be a challenge!)
  why is that?
- Security funding and planning decisions should involve **three distinct groups** of decision makers or "stakeholders“:
- **Stakeholders**:
  1. **Information security community** - protects the information assets of an organization
  2. **Information technology community** - supports the business objectives by supplying and supporting IT that is appropriate to the organization’s needs
  3. **General business community** - articulates and communicates organizational policy and objectives and allocates resources to the other groups

What is Security?

- **Security**: the quality or state of being secure—**to be free from danger**
  - To be ***secure*** is to be ***protected*** from the risk of loss, damage, or unwanted modification, or other hazards (or "threats")
  - **BOTH physical and digital threats** Examples?
    - **ex.** disasters, fires, failures, accidents, hackers)
- **Security** is often achieved by means of **multiple strategies** undertaken simultaneously or used in combination with one another
- **Management's** role is to ensure that **each strategy** is properly planned, organized, staffed, directed, controlled, and FUNDED!
  - Funding challenges with InfoSec? Planning for something that might never happen. Similar concept to insurance, but proactive, not reactive

“It used to be expensive to make things public and cheap to make them private. Now it’s expensive to make things private and cheap to make them public”

Clay Shirky, NYU Professor

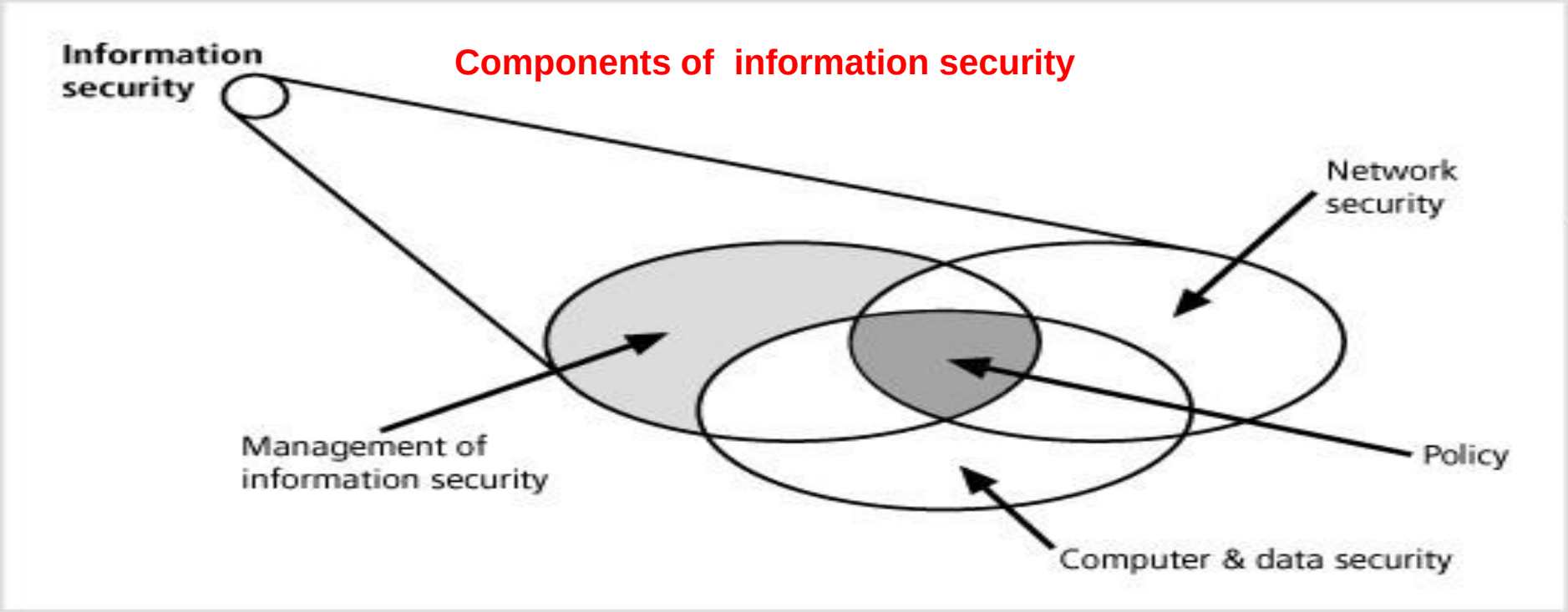
FANSHAWE

What is Security? (continued)

- Specialized areas of security include:
  1. **Physical security** - protecting people, physical assets, and the workplace from various threats
     - Fire, unauthorized access, and natural disasters
  2. **Operations security** - protecting the operations to carry out operational activities without interruption or compromise
  3. **Communications security** - protecting communications media, technology, and content
  4. **Network security** - protecting data networking devices, connections, and contents

What is Information Security?

- **Information security (InfoSec):** the protection of information and its critical elements (confidentiality, integrity and availability), including the systems and hardware that use, store, and transmit that information



The NIST Computer Security Handbook defines the term *Computer Security* as:

"The **protection** afforded to an automated information system in order to attain the applicable objectives of **preserving the integrity, availability and confidentiality** of information system resources" (includes hardware, software, firmware, information/data, and telecommunications).

Key Security Concepts/Objectives

- **Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.**
- Attackers cannot read intercepted messages
- Provided by ***encryption***

- **Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.**
- Assurance that data is not altered
- Provided by ***hashing*** data

- **Ensuring timely and reliable access to and use of information.**
- Network available to all appropriate users
- Provided by ***authentication***

Question: What about Privacy, Identification, Authentication, Authorization, and Accountability? Do these fit into this triad?

Key Concepts of Information Security ***Management***

- **Confidentiality**
  - The characteristic of information whereby **only those with sufficient privileges may access certain information**
  - Measures used to protect confidentiality
    - Access Controls
    - Information classification
    - Secure document storage
    - Application of general security policies
    - Education of information custodians and end users

Key Concepts of Information Security *Management* (cont'd)

- **Integrity**
  - The quality or state of being **whole, complete, and uncorrupted**
- Information integrity is threatened
  - If exposed to corruption, damage, destruction, or other disruption of its authentic state
- Corruption can occur while information is being compiled, stored, or transmitted

Key Concepts of Information Security *Management* (cont'd)

- **Availability**
  - The characteristic of information that enables user access to information in a required format, without interference or obstruction
  - A user in this definition may be either a person **or** another computer system
  - Availability does not imply that the information is accessible to any user, but rather implies availability to **authorized users**

Key Concepts of Information Security

- Identification (Identity Access Management - **IAM**)
  - An information system possesses the characteristic of identification when it is able to recognize individual users
  - Identification and authentication are essential to establishing the level of access or authorization that an individual is granted

  What are they ways you might identify yourself to an information system?

- Triple A (AAA)
  - Authorization (what can you do?)
  - Authentication (aka "verification" – are you who you claim to be?)
  - Accountability (can the activity be traced back to a unique/specific user?)
    - *Explained in the next slide*

Key Concepts of Information Security (cont'd)

- Authentication
  - Occurs when a control proves that a user possesses the identity that he or she claims
- Authorization
  - Assures that the user has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset
  - User may be a person or a computer
  - Authorization occurs after authentication
- Accountability
  - Exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process

Some Key Terms you will see in your readings

Learn to speak the "language of InfoSec"

Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Computer Security Terminology

RFC 4949, *Internet Security Glossary*, May 2000

Active Learning Exercise 1b: Online Flashcards

- This is very useful strategy for learning and studying
- I like Anki, but you can also use Quizlet.com, cram.com, brainscape.com are just a few examples. Or just use a notebook ☺
- **Start your flashcard deck today** and **update it regularly**
- Make it a fun game/competition. Share your card decks and/or stump your peers in the class!

- I am considering bonus marks for the flashcards, but haven't decided yet…
  - **Your thoughts??**

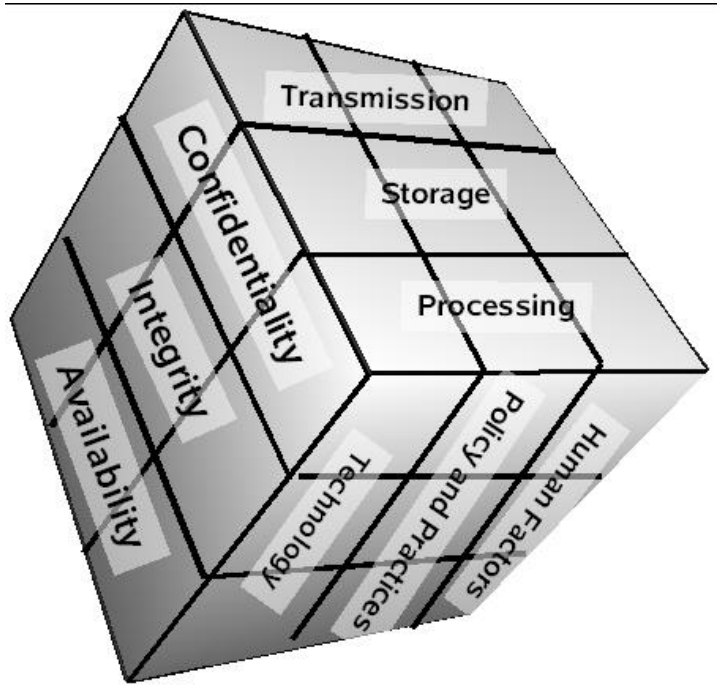
CNSS Security Model

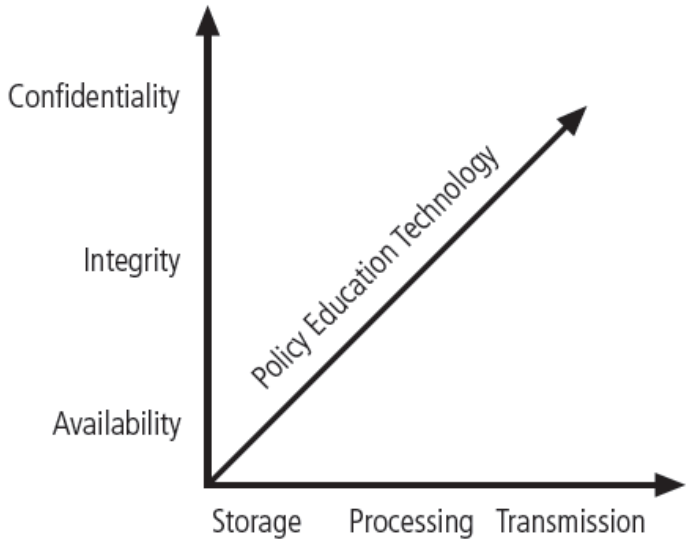
- C.I.A. triangle (also called CIA triad)
  - Confidentiality, integrity, and availability are **primary security objectives**
  - Has expanded into a more comprehensive list of critical characteristics of information

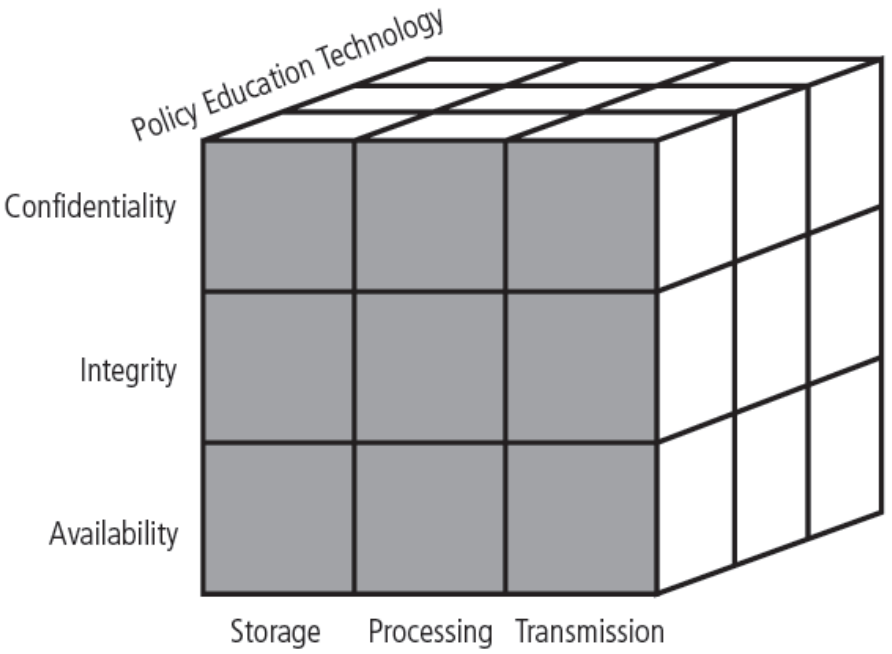
- NSTISSC (now called CNSS) Security Model
  - Also known as the **McCumber Cube**
  - Provides a more detailed perspective on security
  - Covers the three dimensions of information security "interconnectedness" in **each** of the 27 cells

  - **National Security Telecommunications and Information Systems Security Committee** (NSTISSC) became the CNSS - **Committee on National Security Systems**) as per President GW Bush in 2001

CNSS Security Model (cont'd) – McCumber Cube







Source: Course Technology/Cengage Learning
(adapted from NSTISSI No. 4011)

CNSS Security Model (cont'd.)

- Limitations of this model:
  - **Omits** discussion of detailed guidelines and **policies that direct the implementation of controls**
  - Very specific and therefore **restrictive**
  - Weakness of this model emerges if viewed from **a single perspective**
    - Model forces you to include all three communities of interest
      - Ex. Policies, technical controls, user training

What is Management?

FANSHAWE

What is Management?

- **Management is the process of achieving goals and objectives using a given set of resources efficiently and effectively**

- Roles of management?
  - **Informational role** - collecting, processing, and using information that can affect the completion of the objective
  - **Interpersonal role** - interacting with superiors, subordinates, outside stakeholders, and other parties that influence or are influenced by the completion of the task
  - **Decisional role** - selecting from among alternative approaches and resolving conflicts or challenges

Information Security Planning

- What are the qualities of a successful InfoSec Manager!

- Are you be able to demonstrate?:
  - Knowledge retention
  - Critical Thinking
  - Understanding yourself and others
  - Versatility and creativity under adversity
  - Application of learned skills

Behavioral Types of Leaders – “Management Styles”

- Three basic behavioral types:
  - **Autocratic, democratic/consultative, and laissez-faire**
- **Autocratic leaders**
  - reserve all decision-making responsibility for themselves
  - “Do as I say” types of managers
- **Consultative leaders**
  - still make all decisions, but do so after seeking input from all interested parties, requesting ideas and suggestions
- **Laissez-faire**
  - known as the “laid-back” leader, “hands off” style. Does not interfere,
  - Often sits back and allows the process to develop as it goes

Management Characteristics

- **Two basic approaches to management**:
  - *Traditional management theory* - uses the core principles of planning, organizing, staffing, directing, and controlling (POSDC)
  - *Popular management theory* - uses the core principles of **planning, organizing, leading, and controlling (*POLC*)** as management's roles.
- The traditional management theory is often well covered in business courses
  - We will focus on the POLC principles
  - Everyone can lead, but InfoSec managers may not direct (CSO vs CTO vs CISO)
    - CSO – security-focused
    - CTO or CIO – Business operations focused
    - CISO – security & operations focussed

POLC Management Characteristics - Planning

- **Planning** - process of developing, creating, and implementing strategies to accomplish objectives
- setting objectives and how to achieve them “where do we want to be and how will we get there?”
- Three levels of planning:
  - ***Strategic planning*** - occurs at the highest levels of the organization and for a long period of time (more than 5 years)
  - ***Tactical planning*** - focuses on production planning and integrates organizational resources at a level below the entire enterprise (3-5 years)
  - ***Operational planning*** - focuses on the day-to-day operations of local resources and occurs in the present or the short term (daily – one year)

Management Characteristics – Planning (con't)

- Planning begins with the creation of strategic plans for the entire organization
  - Resulting plan is divided into planning elements relevant to each major business unit of the organization
  - Business units create business plans that meet the requirements of the overall organizational strategy with tactical plans
  - Strategic & Tactical Plans are then communicated to mid-level managers and supervisors to create operational plans for each area
  - ***Objective****:* an intermediate point that allows you to measure progress toward the goal

Management Characteristics – Organizing and Leading

- **Organizing**: management function dedicated to the structuring of resources to support the accomplishment of objectives
  - Arranging resources to achieve the business goal
  - Includes the structuring of departments and staff, the storage of raw materials to facilitate manufacturing, and the collection of information
- **Leading**: encouraging the implementation of the planning and organizing functions
  - Influencing people to work towards achieving your objectives
  - Includes supervising employee behavior, performance, attendance, and attitude while ensuring completion of tasks, goals, and objectives

Management Characteristics - Controlling

- **Controlling:** monitoring progress toward completion and making necessary adjustments to achieve desired objectives
  - Evaluating and modifying tasks to determine if objectives are being met/achieved
  - Establishes and ensures the validity of the organization's plan
- The manager ensures that:
  - Performance/Goals are set
  - Sufficient progress is made (using measured to determine effectiveness)
  - Impediments to the completion of the task are identified and resolved
  - No additional resources are required
  - Status Reporting feeds back to Senior Management for action

Solving Problems (as a Manager)

- Step 1: Recognize and define the problem
- Step 2: Gather facts and make assumptions (analyze the problem)
- Step 3: Develop possible solutions – Be creative!
- Step 4: Analyze and compare possible solutions
  - Analysis may include reviewing multiple factors, including economic, technological, behavioral, and operational feasibilities
- Step 5: Select, implement, and evaluate a solution

- Problem Solving becomes an ongoing Process…

Principles of Information Security Management

- The extended characteristics of information security are known as **the six P's**
  1. Planning
  2. Policy
  3. Programs
  4. Protection
  5. People
  6. Projects

  Each of these are explored in the slides to follow…

1. Planning

- Planning as part of InfoSec management
  - An extension of the basic planning model discussed earlier
- Included in the InfoSec planning model
  - Activities necessary to support the design, creation, and implementation of information security strategies

1. Planning (cont'd)

- **Types of InfoSec plans**
  - Business continuity planning (BCM – Business Continuity Management)
  - Incident response planning (BIA – Business Impact Analysis)
  - Disaster recovery planning (DRP)
  - Policy planning
  - Personnel planning (HRM – Human Resource Management)
  - Technology rollout planning
  - Risk management planning (BCP)
  - Security program planning
    - includes education, training and awareness

2. Policy

- **Policy: the set of organizational guidelines that dictates certain behavior within the organization**
- Three general policy categories:
  - *Enterprise information security policy (**EISP**)* - sets the tone for the InfoSec department
  - *Issue-specific security policy (**ISSP**)* - sets of rules that define acceptable behavior within a specific technology
  - *System-specific policies (**SysSPs**)* - control the configuration and/or use of a piece of equipment or technology

3. Programs

- **Programs**: InfoSec operations that are specifically managed as separate entities
  - Example: a security education training and awareness (SETA) program
- Other types of programs
  - Physical security program
    - complete with fire protection, physical access, gates, guards, etc.
  - Programs dedicated client/customer privacy and awareness

4. People

- People
  - **The most critical link in the information security program**
  - Managers must recognize the crucial role that people play in the information security program
  - This area of InfoSec includes security personnel and the security of personnel, as well as aspects of a SETA program
  - **73% of Security breaches can be traced to human error (CIO magazine 2011)**

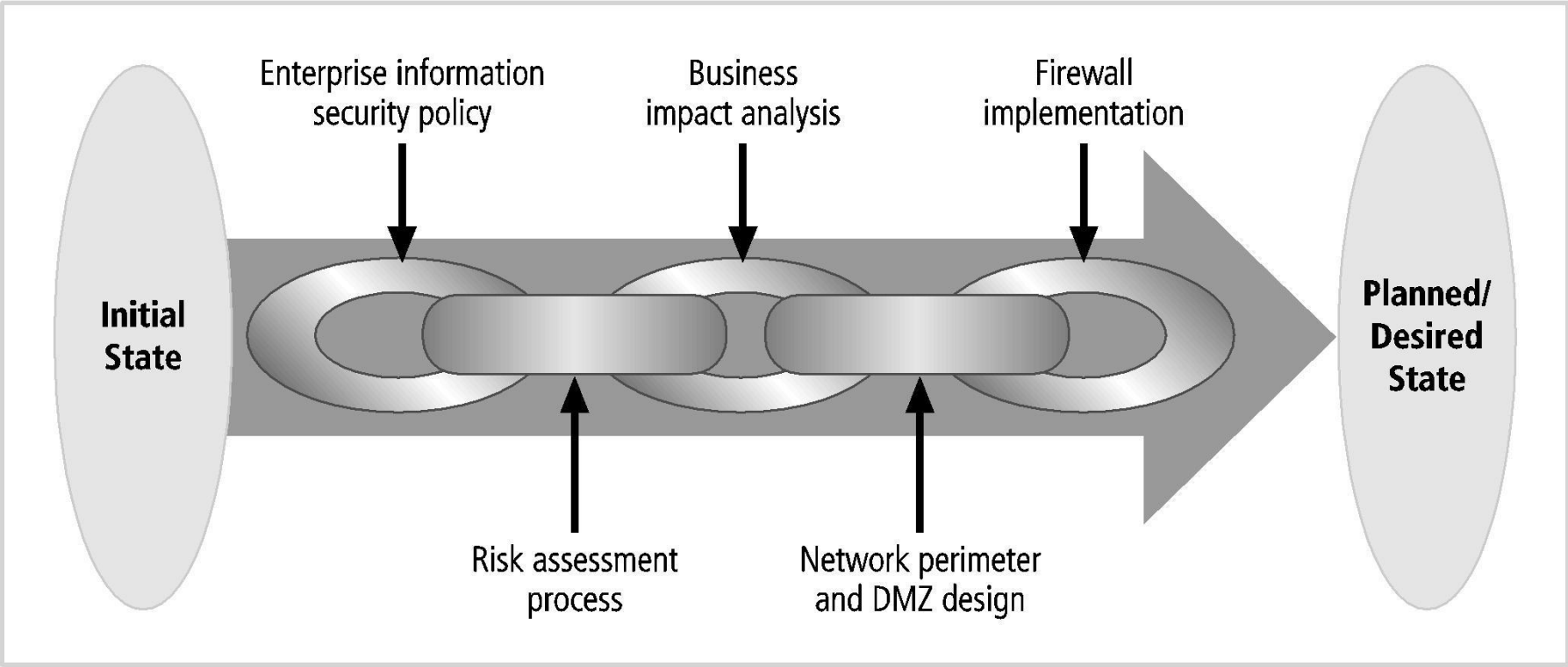
5. Protection

- Executed through risk management activities
  - Including risk assessment and control, protection mechanisms, technologies, and tools
  - Each of these mechanisms represents some aspect of the management of specific controls in the overall information security plan

6. Project Management

- Project management
  - Identifying and controlling the resources applied to the project
  - Measuring progress
  - Adjusting the process as progress is made
- Information security is a process, not a project
  - Each element of an information security program must be managed as a project
  - A continuous series, or chain, of projects
- Some aspects of information security are not project based
  - They are managed processes (operations)
  - Ad-hoc or emergency response

Project Management (cont'd.)



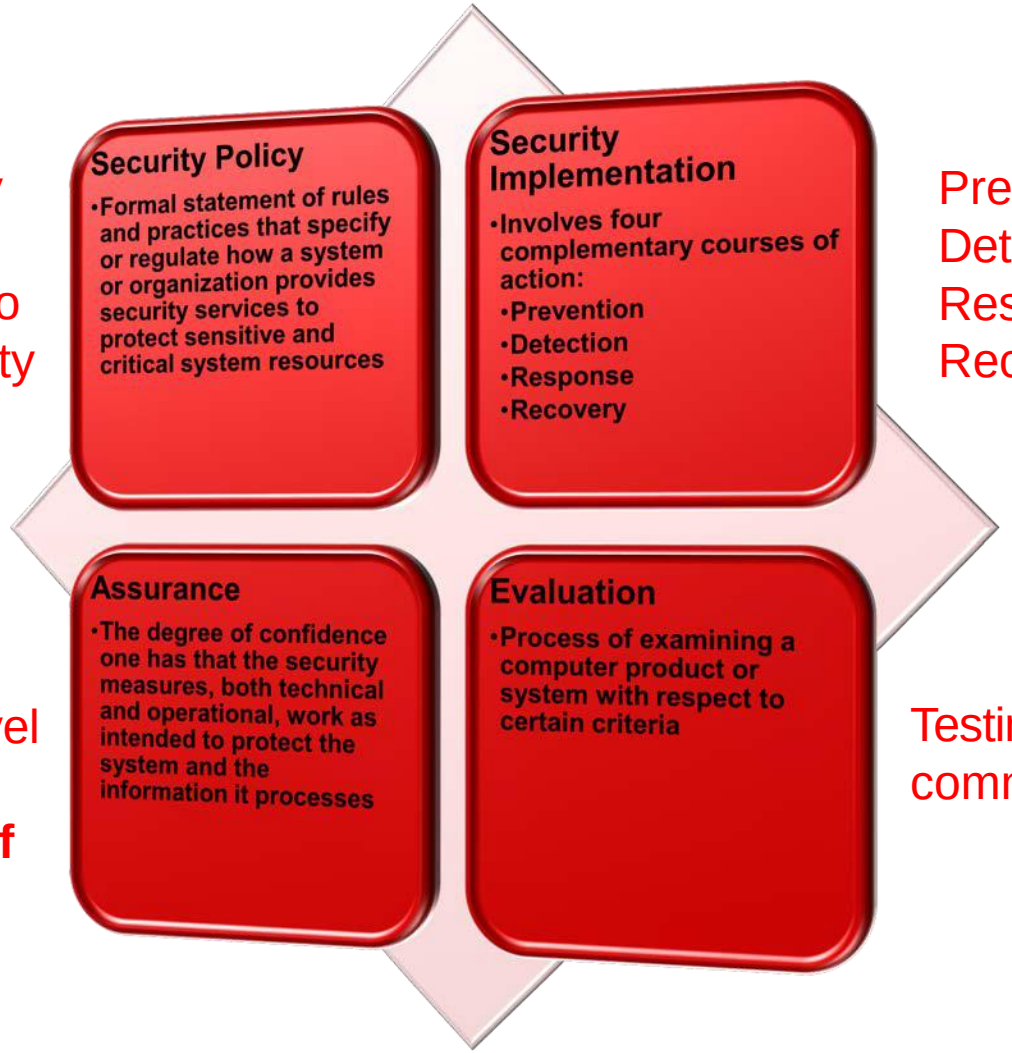
Source: Course Technology/Cengage Learning

ISMS

- ISMS – Information Security Management System
- Is a formal, controlled set of processes and procedures that deals with security within an organization. It ties **people, processes and technology together along with policy** all within a system
- ISO27000 series of standards
- Code of Practice for Information Security Management
- The model is Plan, Do, Check, Act

Computer Security Strategy

The first step in devising security services and mechanisms is to develop a security policy.



Prevention
Detection
Response
Recovery

Assurance measured in level of **confidence**, not formal **proof**

Testing against a set of common criteria

References/Readings:

- Computer Security – Principles & Practices (4th Ed.) (Stallings & Brown)
- Management of Information Security (Whitman & Mattord)
- ISO27000 series of Standards.

For Next Class:

- Get the textbook and start reading ☺
  - Read Chapter 1 of course textbook
  - Chapter 14 if possible before next class.
- Next week we will be discussing
  - What is Risk? How do we identify risks?
  - What is a BIA