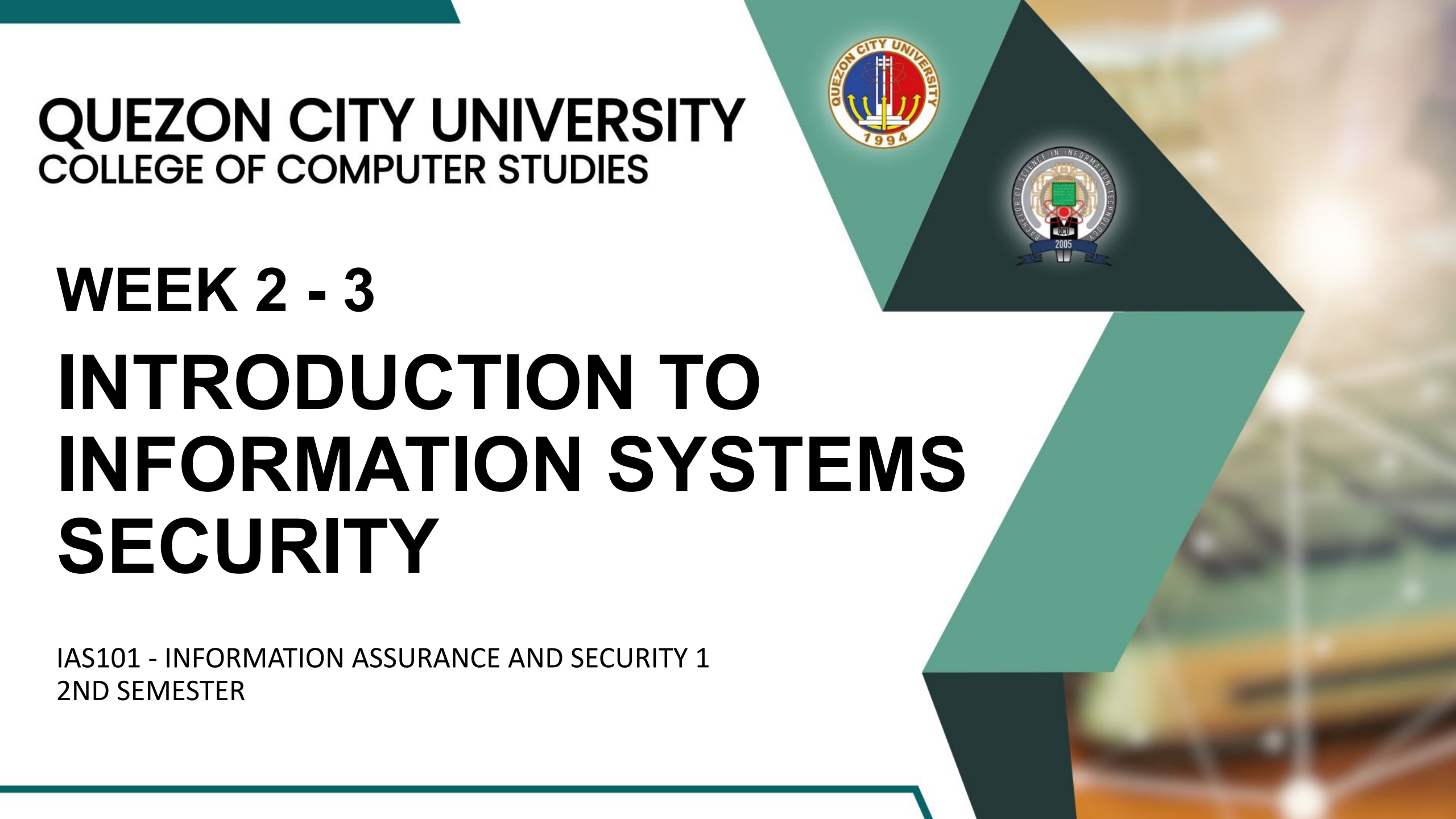
QUEZON CITY UNIVERSITY
COLLEGE OF COMPUTER STUDIES

WEEK 2 - 3

INTRODUCTION TO INFORMATION SYSTEMS SECURITY

IAS101 - INFORMATION ASSURANCE AND SECURITY 1
2ND SEMESTER



LEARNING OUTCOMES:

At the end of the session, the students should be able to:

- Explain information systems and security and its effect on people and businesses
- Relate how availability, integrity, and confidentiality affect the seven domains of IT infrastructure
- Describe the threats and vulnerabilities within the seven domains
- Determine the purpose of IT security policy framework in reducing risk.

Importance of Information

- Information is valuable therefore, Information Systems are valuable, and compromising Information Security Services (C-I-A) have real consequences (loss).

- **Confidentiality:** death, proprietary information, privacy, theft
- **Integrity:** theft, loss of confidence, validity
- **Availability:** lost productivity, disruption of C2, defense, emergency services.

Concepts

- Information **Systems**

  System that stores, transmit, and process information.

- Information **Security**

  The protection of information.

- Information **Systems Security**

  The protection of systems that store, transmit, and process information.

Fundamental Concepts

- What is Information Assurance (IA)?

  - it is our assurance (confidence) in the protection of our information / Information Security Services.

- What are Information Security Services (ISS)?

  - Confidentiality
  - Integrity
  - Availability

Information Security Services (ISS)

- **Confidentiality**
  - Making sure our information is protected from unauthorized disclosure.

- **Integrity**
  - Making sure the information we process, transmit, and store has not been corrupted or adversely manipulated.

- **Availability**
  - Making sure that the information is there when we need it and gets to those who need it.

Private vs. Military Requirements

- Which security model an organization uses depends on its goals and objectives.

- Military is generally concerned with CONFIDENTIALITY

- Private businesses are generally concerned with AVAILABILITY (ex. Netflix, eBay) or INTEGRITY (ex. Banks)

- Some private sector companies are concerned with CONFIDENTIALITY (ex. Hospitals)

Fundamental Concepts

- What is Cyberspace?

  - The term adopted by the USG

  - The virtual environment of information and interactions between people.

  - Telecommunications Network Infrastructure

  - Information Systems

  - Internet

Review of Fundamental Concepts

- What is the Defense in Depth Strategy?

  - an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information.

- People, Technology, Operations

Defense in Depth Layered Security

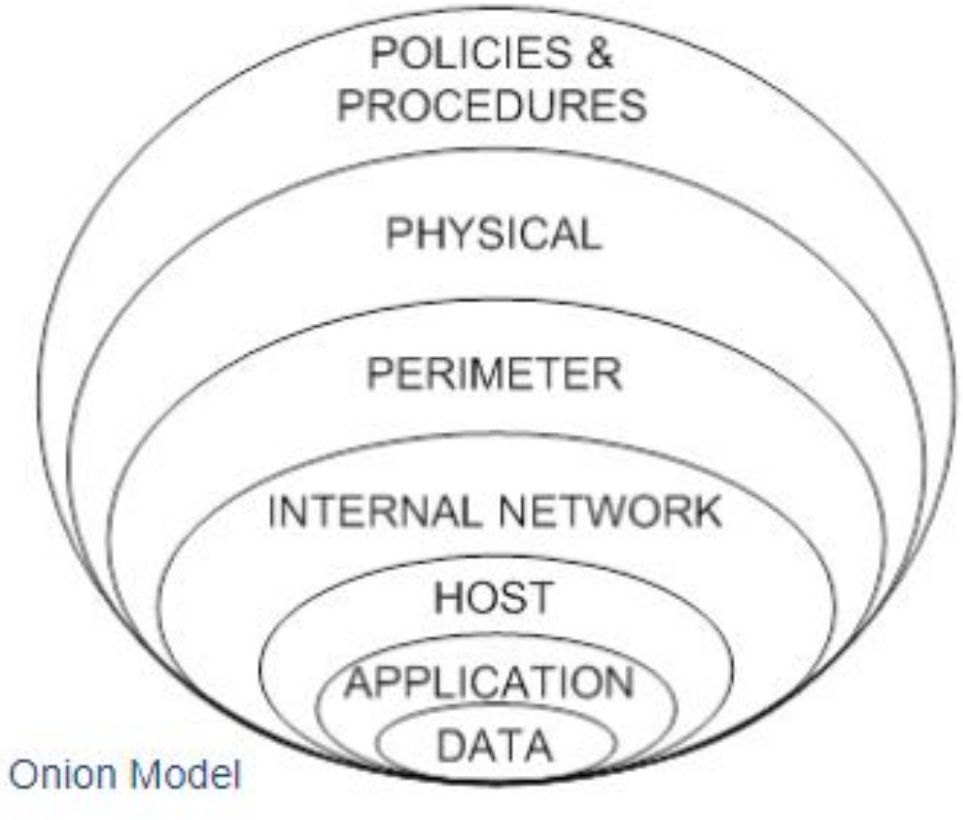


Figure 1: Defense in Depth Layered Security

Information Systems Security: Privacy

- Defined: the protection and proper handling of sensitive information

- Requires proper technology for protection

- Requires processes and controls for appropriate handling

Personal Identifiable Information: PII

- Name
- Social Security Number
- Phone Number
- Driver's License Number
- Credit Card Numbers
- Etc.

Risk Management

- Information Systems Risk Management is the process of identifying, assessing, and mitigating (reducing) risks to an acceptable level.

Why is this important?

- There is no such thing as 100% security.

Risk Management

- Risk must be identified, classified and analyzed to assess potential damage (loss) to company.

- Risk is difficult to measure and quantify, however, we must prioritize the risks and attempt to address them.

Eliminating Risk

- Identify assets and their values.
- Identify vulnerabilities and threats.
- Quantify the probability of damage and cost of damage.
- Implement *cost effective* countermeasures.

Computer Network Defense

- Defensing against unauthorized actions that would compromise or cripple information systems and networks.

- Protect, monitor, analyze, detect, and respond to network attacks, intrusions, or disruptions.

General Security Concepts

- CIA Triad (Information Security Concepts)

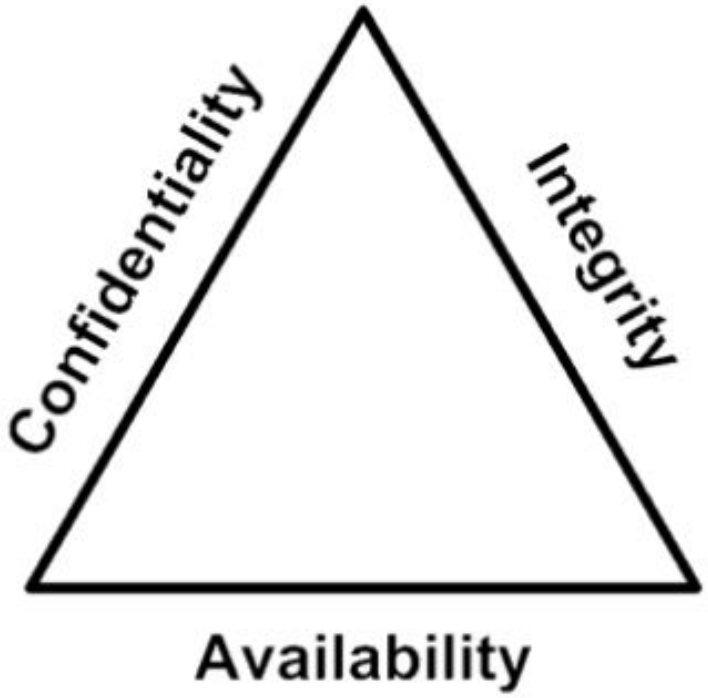


Figure 2: CIA Triad

General Security Concepts

- Operational Model of Computer Security

Protection = Prevention + Detection + Response

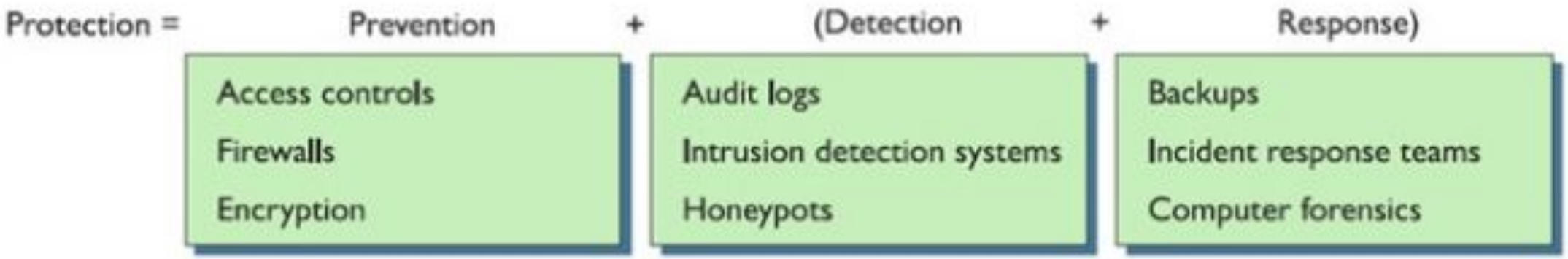


Figure 3: Operational Model of Computer Security

General Security Concepts

Security Principles

- Least Privilege (Need to Know)
  - Users should have only the necessary (minimum) rights, privileges, or information to perform their tasks (no additional permission)

- Implicit Deny
  - "Deny all" authorization and access (backlisted) unless specifically allowed (white list)
  - Default security rule for firewalls, routers, etc.

General Security Concepts

Security Practices

- Separation of Duties
  - Ensures tasks are broken down and are accomplished / involve by more than one individual.
  - Check and balance system.

- Job Rotation
  - Rotation individuals through jobs/tasks.
  - Organization does not become dependent on a single employee.

General Security Concepts

Security Practices

- Economy Mechanism
  - Described as always using simple solutions when available.
  - Protection mechanism should be small and simple.

- Complete mediation
  - Refers to the concept that each and every request should be verified.

General Security Concepts

Security Practices

- Least common mechanism
  - States the mechanisms used to access resources should be dedicated and not shared.

- Psychological acceptability
  - Refers to the users' acceptance of security measures.

General Security Concepts

Layered Security

- Defense in Depth
- Redundancy
- No single point of Failure

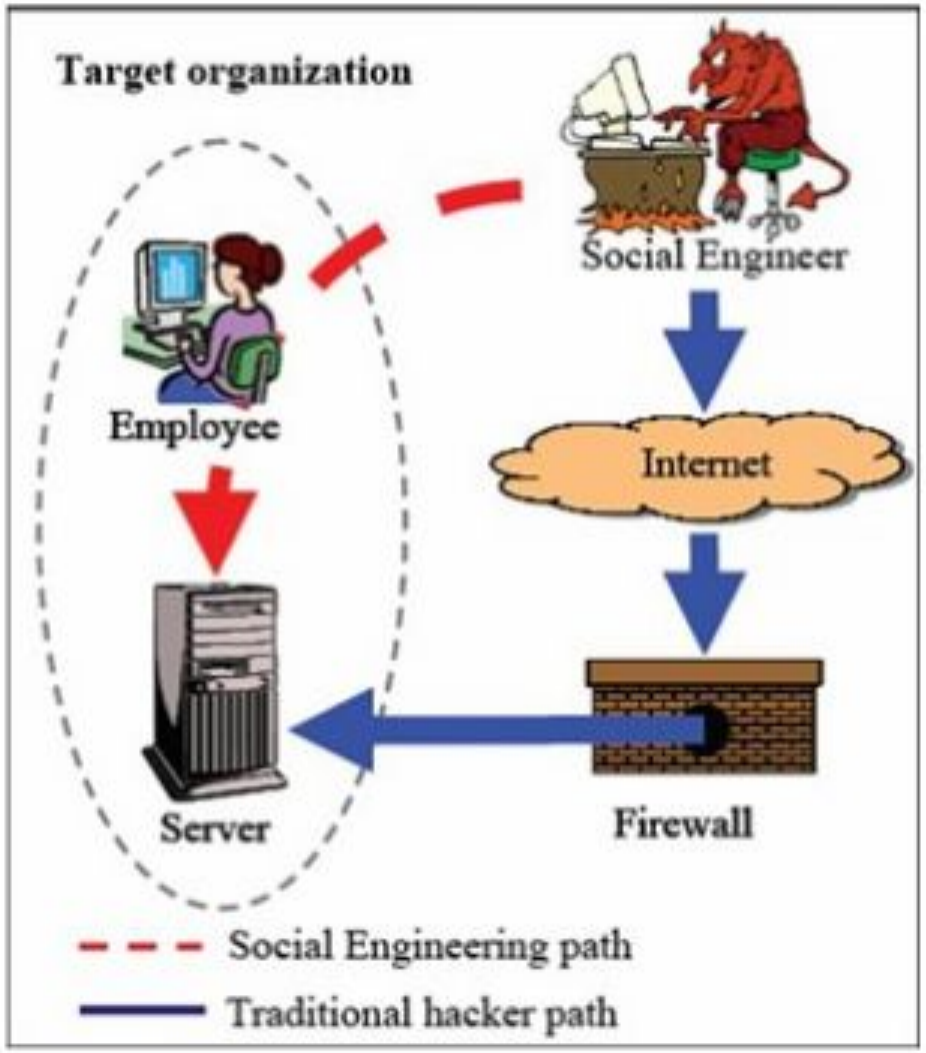
General Security Concepts

- Access
  - Control what a subject can perform or what objects the subject can interact.
  - i.e. Access Control List (ACL's)

- Authentication
  - Verify the identity of a subject. (Who You Are)
  - Involves identification
  - Passwords, cards, biometrics (fingerprints), etc.
  - Digital Certificates

General Security Concepts

- Authorization
  - Verifies what a subject is authorized to do.
- Social Engineering
  - Talk individuals into divulging information that they normally would never have.
  - Used to gain information on identities, access, or authorization.
  - Data aggregation.



General Security Concepts

- Policies
  - Constraints of behavior on systems and people
  - Specifies activities that are required, limited, and forbidden

Example:

- Information systems should be configured to require good security practices in the selection and use of passwords.

General Security Concepts

- Requirements
  - Required characteristics of a system or process
  - Often the same as or similar to the policy
  - Specifies what should be done, not how to do it.

  Example:
  - Information systems must enforce password quality standards.

- Guidelines define how to support a policy
  - Example: ‘as a guideline’ passwords should not be dictionary words, don’t write passwords down, etc.

General Security Concepts

- Standards
  - What products, technical methods will be used to support policy

  Example:
  - All fiber optics cable must be ACME brand
  - Passwords must be at least 8 characters, contain 2 upper and lower case characters.

- Procedure
  - Step by step instructions

General Security Concepts

- Classifications of Information
  - Sensitivity / Confidentiality

Example:
- Unclassified (UNCLASS)
- For Official Use Only (FOUO)
- Confidential
- Secret (S)
- Secret Releasable (S//REL)
- Top Secret (TS)

WEEK 3

Seven Domain of a Typical IT Infrastructure

- User Domain
- Workstation Domain
- LAN Domain
- LAN-to-WAN Domain
- WAN Domain
- Remote Access Domain
- System / Application Domain

User Domain

- The User Domain includes people or employees.
- An HR department maintains records on employees.
- These can be manual records, such as folders held in filing cabinets, or files held on servers.

Data on Users includes:

- Personal and contact data
- Employee reviews
- Salary and bonus data
- Health care choices

Workstation Domain

- It includes PC's used by employees either typical desktop PC's, mobile computers, or laptops.

Assets in the Workstation Domain have Two Risks to Address:

1. **Theft**

- an organization has a significant investment in these systems.

- Inventory management systems include processes where each item is manually located on a periodic basis.

- this verifies the system is still in the organization's control.

Workstation Domain

2. **Updates**

- As updates, fixes, and patches are released, they need to be applied to the systems.

- If the systems are not updated, they become vulnerable to new exploits. Use automated asset management system to keep systems up to date. An automated system will often perform three steps:

1. Inspect systems for current updates,

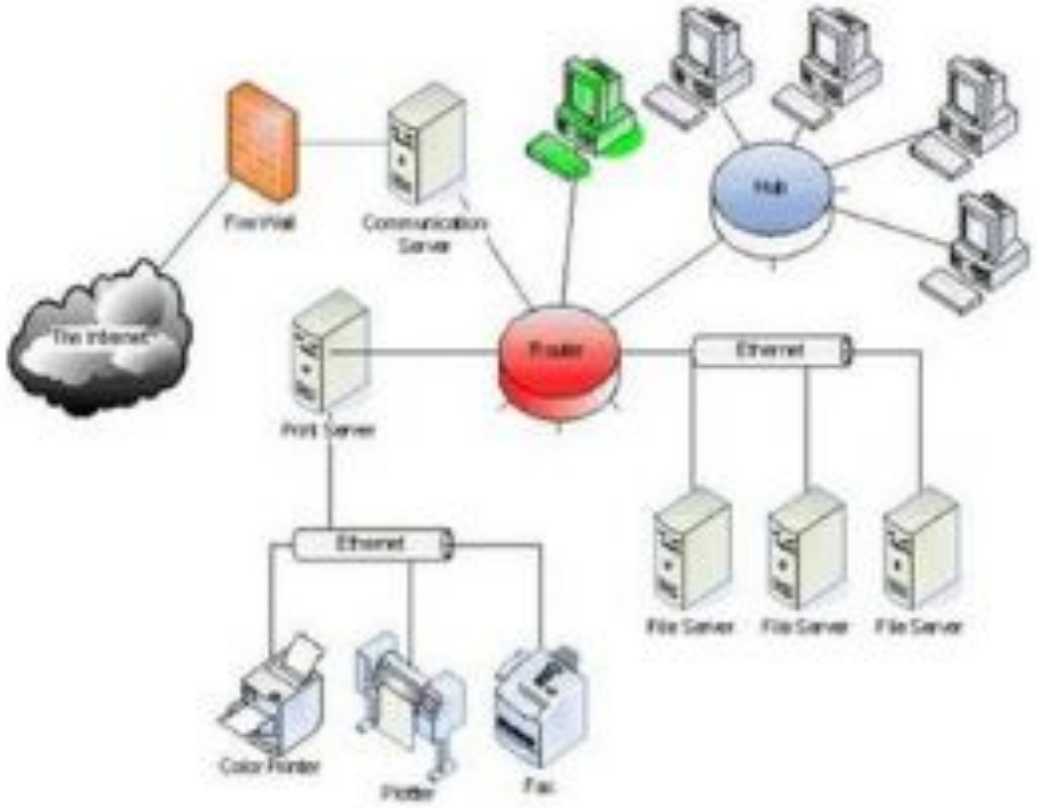
2. Apply updates, and

3. Verify the updates.

.

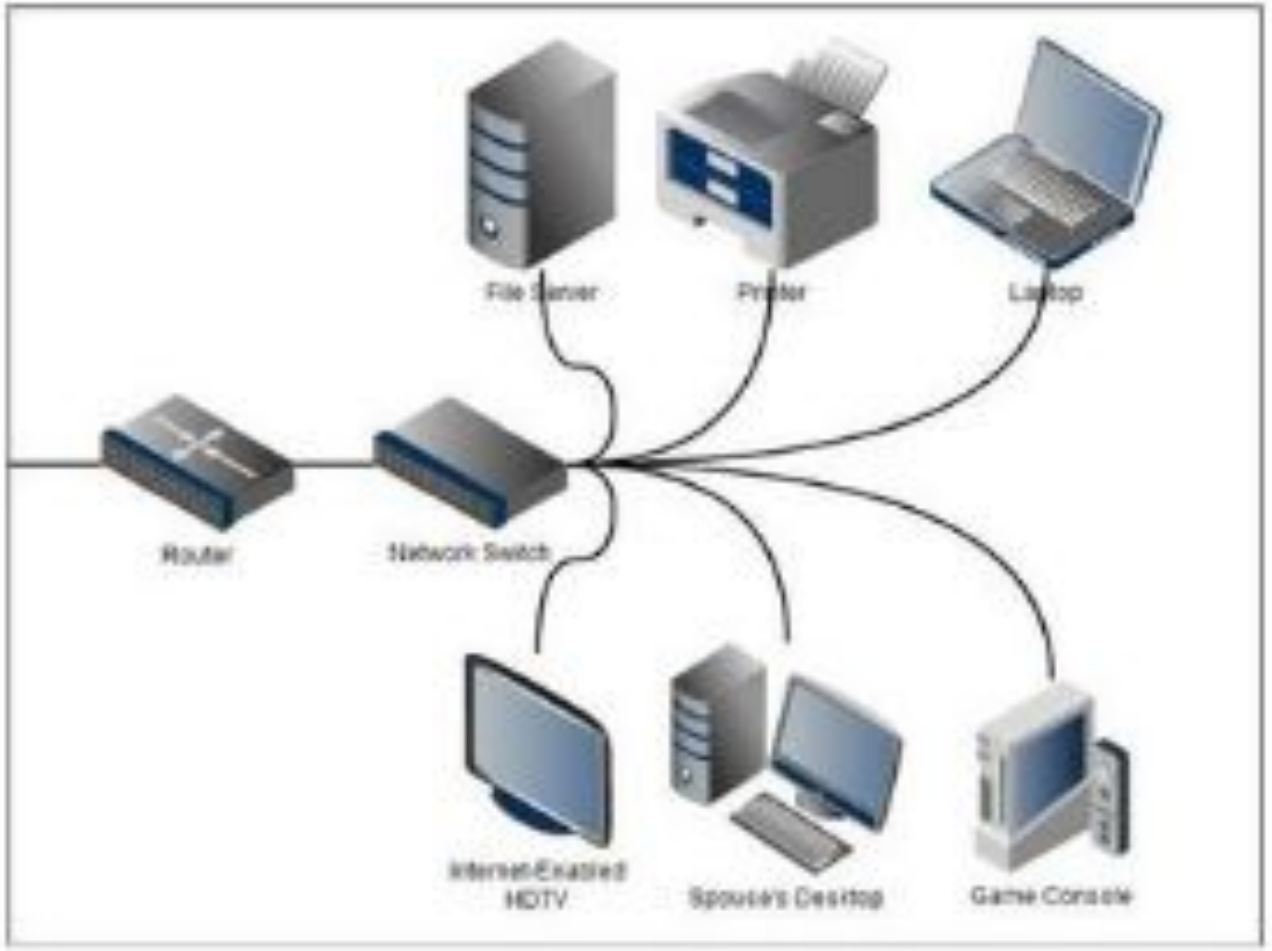
LAN Domain

- It includes all the elements used to connect systems and servers together. The Local Are Network (LAN) is internal to the organization.
- The primary hardware components are hubs, switches, and routers.



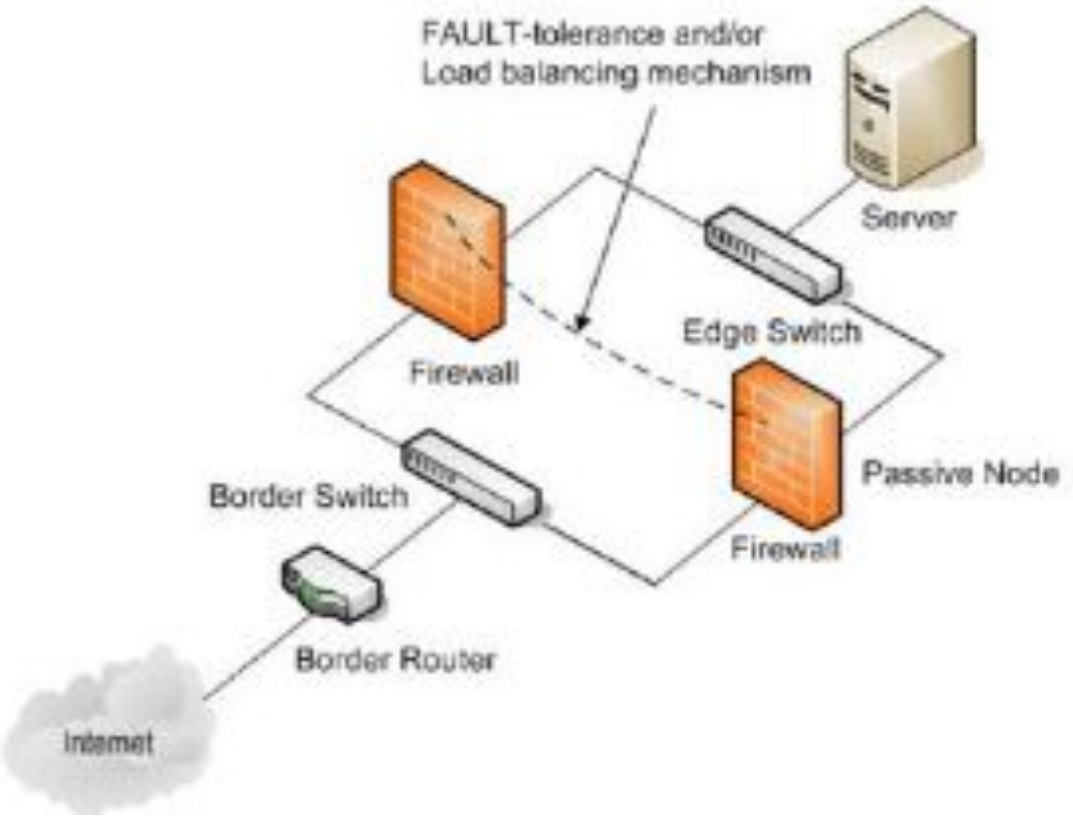
LAN Domain

- It is important to have a basic inventory of these devices.
- This includes the basics such as model, serial number, and location.
- Although any network device includes firmware, the more functional network devices such as routers and switches have a built-in operation system (OS).



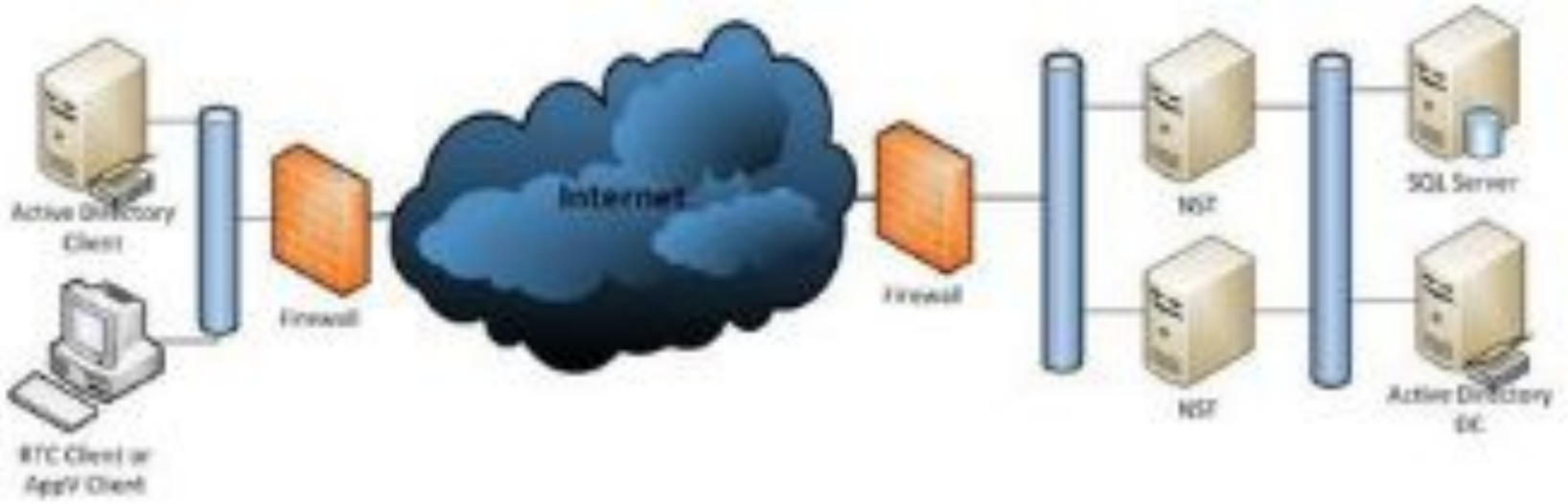
LAN to WAN Domain

- LAN to WAN Domain is the area where your internal LAN connects to the Wide Area Network (WAN).
- In this context, the WAN is often the Internet.
- The primary devices you're concerned with here are the **Firewalls**.
  - ✔ single firewall separating the LAN from the WAN.
  - ✔ multiple firewalls to create a demilitarized zone (DMZ) or a buffer area.



WAN Domain

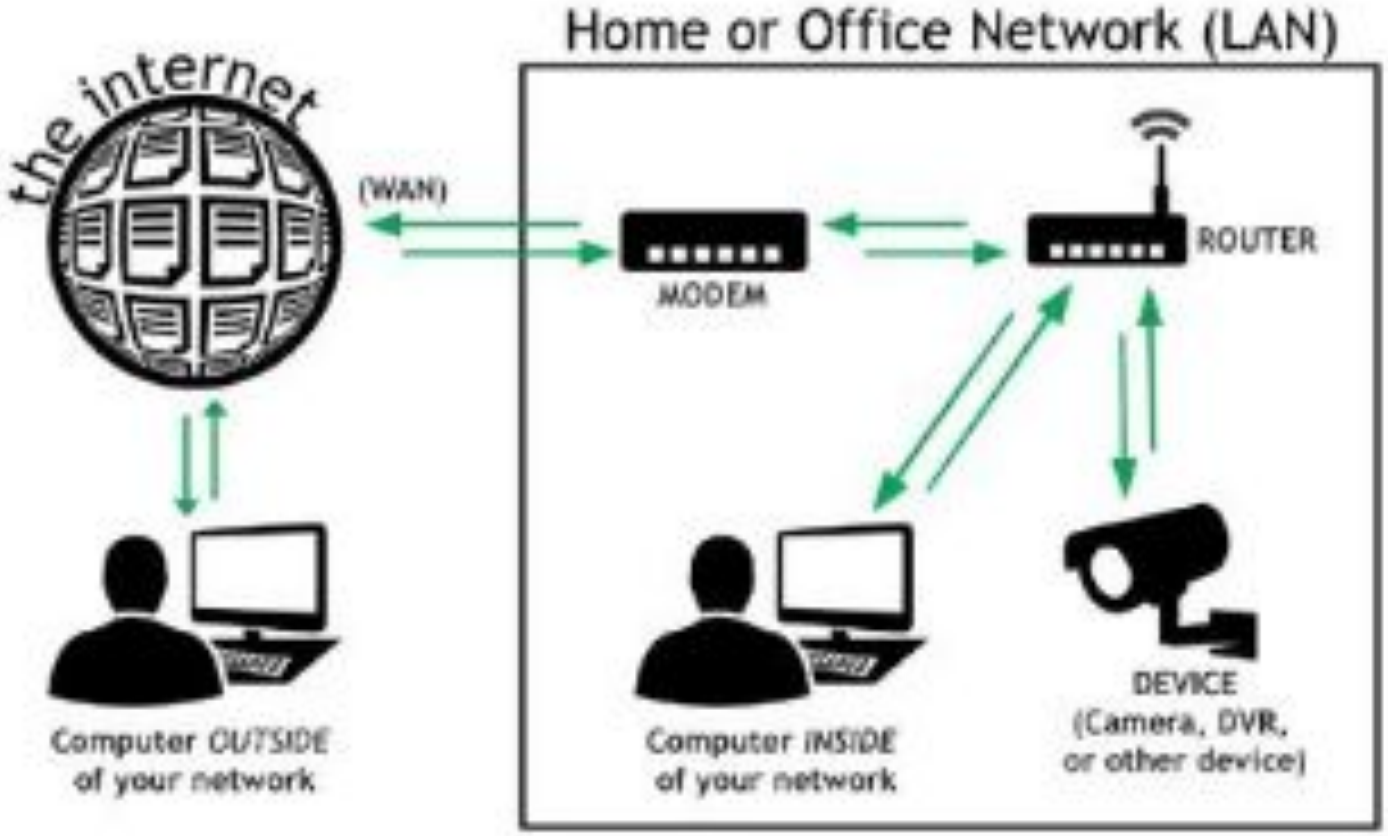
- The WAN domain includes any servers that have direct access to the Internet.
- This includes any server that has a public Internet Protocol (IP) address.



Remote Access Domain

- Remote Access technologies give users access to an internal network via an external location.
- This can be done via direct dial-up or virtual private network (VPN).
  - **Dial-up** – when used, clients and servers have modems and access to phone lines.
  - **VPN** – when used, the VPN server has a public IP address available on the Internet.
- Client access the internet, and then use tunneling protocols to access the VPN servers.

Remote Access Domain



System / Application Domain

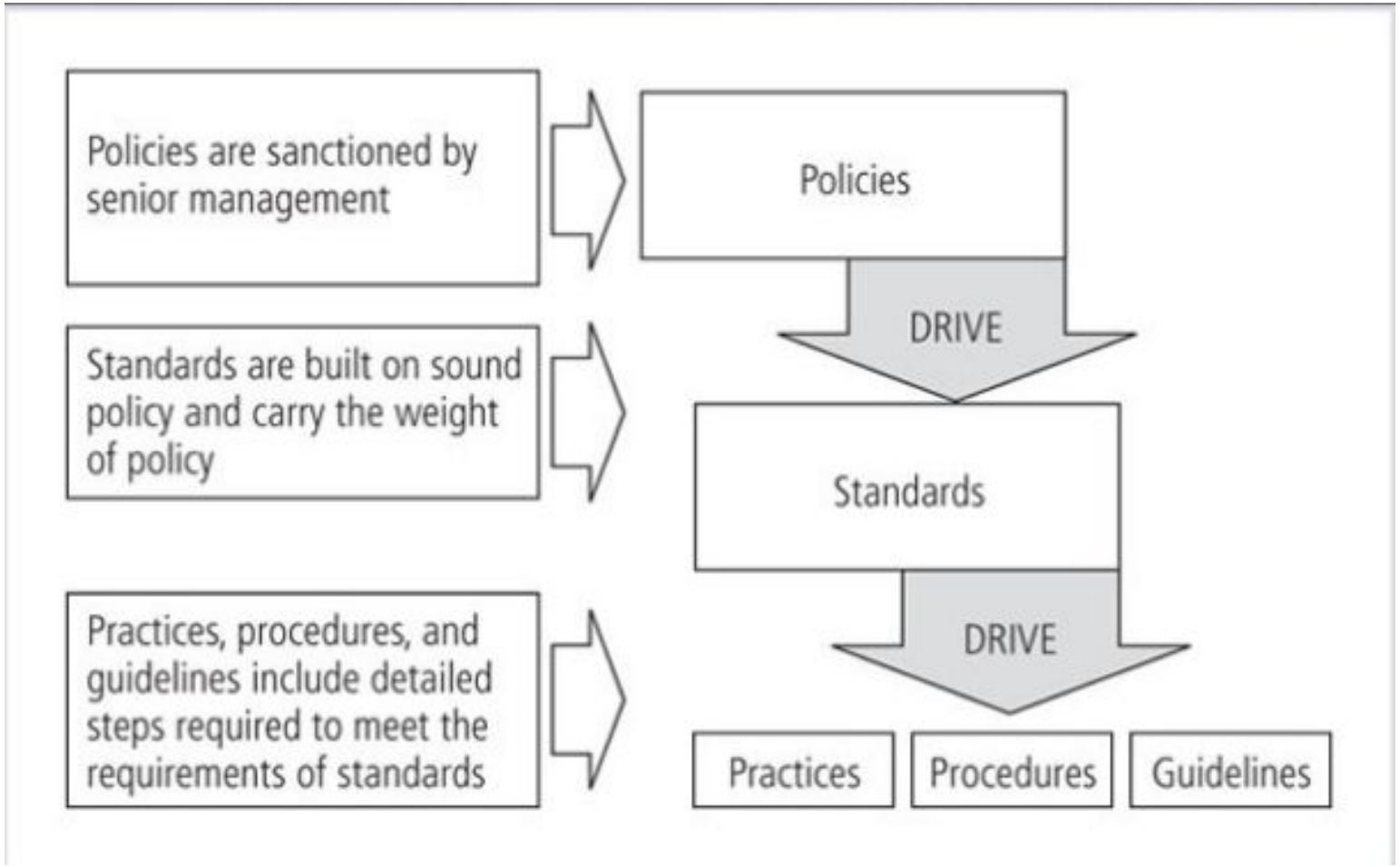
- It includes servers used to host server applications. Some examples of different types of application server includes:
  - **E-mail servers –** this can be a single e-mail server. It can also be a larger e-mail solution, including both front-end and back-end server configurations.
  - **Database servers –** this can be an Oracle or Microsoft SQL server. It can be a single server or a group of servers.
  - **Web Servers –** It host web sites and serve them to Web clients. A single web server can host a single Web site or hundreds of Websites.

Information Security Policy

- Policy is the essential foundation of an effective information security program.

"The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems"

Policy, Standards, Practices



Guidelines for Effective Policy

- Developed using industry-accepted practices
- Distributed or disseminated using all appropriate methods
- Reviewed or read by all employees
- Understood by all employees
- Formally agreed to by act or assertion
- Uniformly applied and enforced

Developing Information Security Policy

- It is often useful to view policy development as a two-part project
  - Frist, design and develop the policy (or redesign and rewrite an outdated policy)
  - Second, establish management processes to perpetuate the policy within the organization.

- The former is an exercise in project management, while the latter requires adherence to good business practices.

Developing Information Security Policy

- Policy development projects should be
  - Well planned
  - Properly funded
  - Aggressively managed to ensure that is completed on time and within budget.

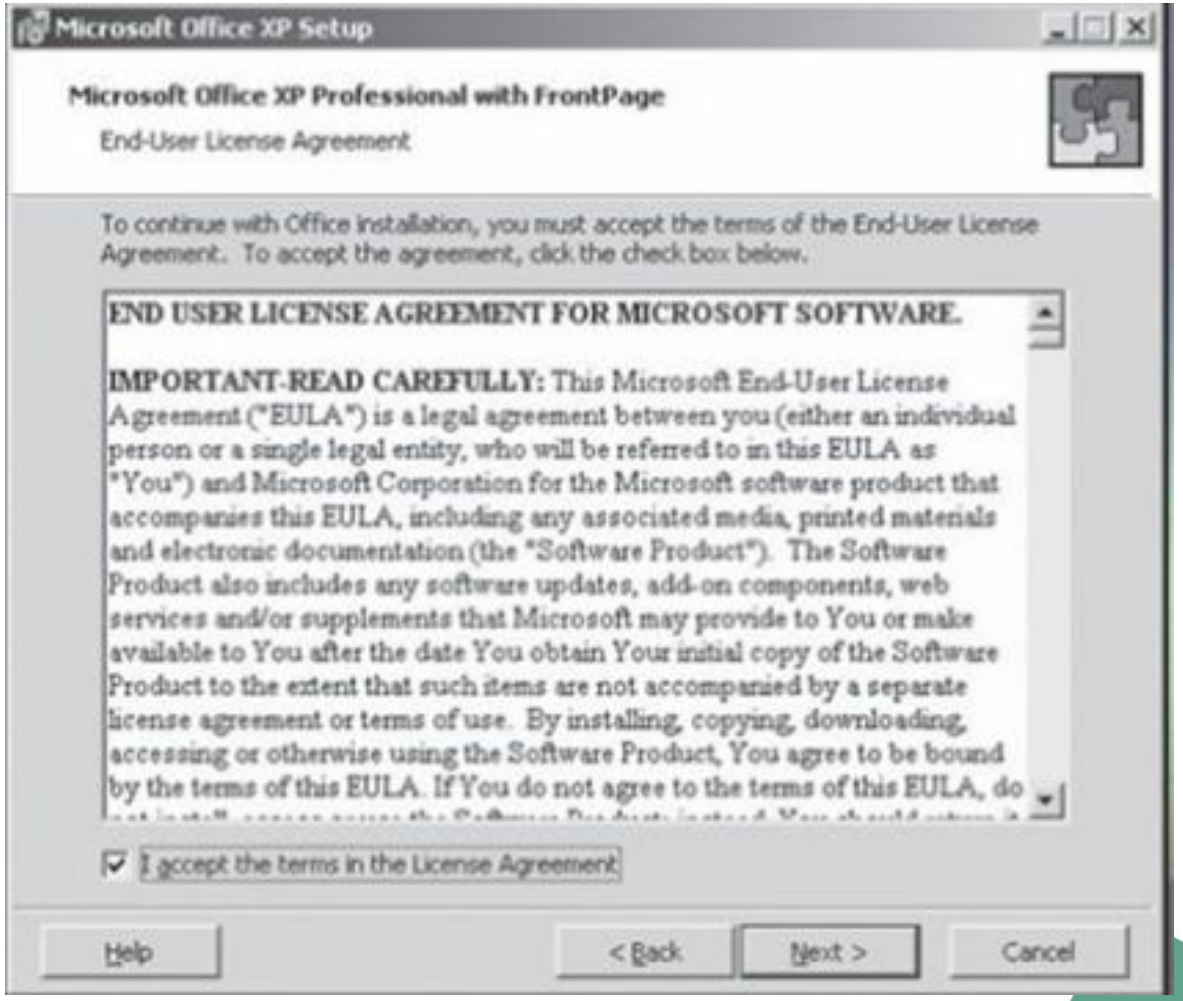
- The policy development project can be guided by the SecSDLC process.

Developing Information Security Policy

- Investigation Phase
  - Obtain support from senior management, and active involvement of IT management, specifically the CIO
  - Clearly articulate the goals of the policy project
  - Gain participation of correct individuals affected by the recommended policies
  - Involve legal human resources and end-users
  - Assign a project champion with sufficient stature and prestige
  - Acquire a capable project manager
  - Develop a detailed outline of and sound estimates for project cost and scheduling.

Developing Information Security Policy

- Analysis Phase should produce
  - New or recent risk assessment or IT audit documenting the current information security needs of the organization.
  - Key reference materials
    * including any existing policies



Developing Information Security Policy

- Design Phase includes

  - How the policies will be distributed
  - How verification of the distribution will be accomplished
  - Specifications for any automated tools
  - Revisions to feasibility analysis reports based on improved costs and benefits as the design is clarified.

Developing Information Security Policy

- Implementation Phase includes
  - Writing the policies

    * Making certain the policies are enforceable as written
    * Policy distribution is not always straightforward
    * effective policy is written at a reasonable reading level, and attempts to minimize technical jargon and management terminology

Developing Information Security Policy

- Maintenance Phase

  - Maintain and modify the policy as needed to ensure that it remains effective as tool to meet changing threats
  - The policy should have a built-in mechanisms via which users can report problems with the policy, preferably anonymously
  - Periodic review should be built in to the process

Summary:

- Information Assurance (AI) is our assurance (confidence) in the protection of our information / Information Security Services.
- ISS is composed of CIA.
- Defense in depth strategy is using layers of defense as protection.
- Risk management is important because there is no such thing as 100% security, and there are several ways to eliminate risks.
- User Domains includes people or employees.
- Workstation domains includes PC's used by employees either typical desktop PC's, mobile computers, or laptops.

Summary:

- LAN domain includes all the elements used to connect systems and servers together.
- LAN to WAN Domain is the area where your internal LAN connects to the Wide Area Network (WAN).
- The WAN domain includes any servers that have direct access to the Internet.
- Remote Access technologies give users access to an internal network via an external location.

Summary:

- Policy is the essential foundation of an effective information security program.
- The objectives of making a policy are to reduced risk, compliance with laws and regulations, and the assurance of operational continuity, information integrity, and confidentiality.
- Enterprise Information Security Program, Issue-specific Information Security, and System-specific are the three types of Information Security Policy.
- There are different guidelines for developing an effective policy.
- The policy development project can be guided by the SecSDLC process.

END OF PRESENTATION.

THANK YOU!