INFORMATION ASSURANCE and SECURITY 2 REVIEWER

NOTE:

- Di kasama ang mga notes here.

Might be in the midterm exam: (sinabi nya yan nung nag lecture sya)

- **CSMA/CA (Carrier -Sense Multiple Access w/ Collision Avoidance)** - Prevents data collisions in wireless networks
- **CSMA/CD (Carrier-Sense Multiple Access w/ Collision Detection)** - Detects and manages collisions in wired networks
- **Daisy Chain** – Devices connected in sequence (up to 9; used by Apple)
- **Redundant Server** – Backup that runs simultaneously for reliability
- **Backup Server** – Activates only when the main server fails
- **DATA** is not **INFORMATION**
- **2 Connectors of RJ45, RJ11:**

  1. RJ45 (Registered Jack 45)
  - **Type:** 8-pin connector.
  - **Used for: Ethernet networking (LAN)**.
  - **Cable Type:** Twisted pair cables (Cat5e, Cat6, etc.).
  - **Function:** Connects computers, routers, and switches in wired networks.

  2. RJ11 (Registered Jack 11)
  - **Type:** 4-pin or 6-pin connector.
  - **Used for: Telephone lines** and **DSL connections**.
  - **Cable Type:** Twisted pair cables (smaller than RJ45).
  - **Function:** Connects telephones and modems to wall jacks.
- **3 Connectors of Fiber Optics**

1. **ST Connector (Straight Tip) -** Uses a bayonet-style twist lock; commonly used in network backbones and data centers.
2. **SC Connector (Subscriber / Square Connector) -** Push-pull connector with square body; provides stable and reliable connections; used in telecom and datacom.
3. **LC Connector (Lucent Connector) –** Small form-factor connector; ideal for high-density connections; used in modern fiber equipment

---

CHAPTER 1: Introduction to the Management of Information Security (based on 3rd edition)

Introduction:

🔷 **Importance of Information Security**

- Protects the organization's most valuable resource: **information assets**.
- Ensures continuity, privacy, and integrity of business operations.
- Businesses now create specialized roles (e.g., Information Security Managers) to manage security.

🔷 **Three Communities of Interest in Information Security**

To make effective security decisions, three groups must collaborate:

1. **Information Security Managers and Professionals**
   - Protect information assets from internal and external threats.
2. **IT Managers and Professionals**
   - Provide and maintain the technology that supports business goals.

3. **Nontechnical Business Managers and Professionals**
    - Set organizational policies, objectives, and allocate necessary resources.

🔷 **Collaboration and Decision-Making**

- These three groups must **work together and reach consensus** on security planning.
- Effective protection of information assets requires **constructive debate and cooperation**. **Information Security as Risk Management**
- Core concept: **Information security = managing risk**.
- Involves identifying, measuring, mitigating, or documenting risks to information assets.
- Leadership from all three communities must support initiatives to control these risks.

What is Security?

🔷 **Understanding Security**

- **Security** means **"the quality or state of being secure—free from danger."**
- To be secure is to be **protected from adversaries, threats, or hazards**.
- Achieving security requires a **multilayered system**—no single solution is enough.
- **Multiple strategies** are often used together to protect assets and ensure continuity.

🔷 **Management's Role in Security**

- Management must ensure that every security strategy is:
    - **Planned**
    - **Organized**
    - **Staffed**
    - **Directed**
    - **Controlled**
- Security is not just a technical process—it requires **effective leadership and coordination**.

🔷 **Specialized Areas of Security**

Each area contributes to the overall **information security program**:

1. **Physical Security** – Protects people, physical assets, and facilities from threats like fire, theft, or natural disasters.
2. **Operations Security** – Ensures business activities can continue without interruption or compromise.
3. **Communications Security** – Protects the organization's communication media, technology, and content.
4. **Network Security** – Protects data networks, connections, and information transmitted across them.

🔷 **Definition of Information Security (InfoSec)**

According to the **Committee on National Security Systems (CNSS)**:

> **Information Security (InfoSec)** is the **protection of information and its critical characteristics—confidentiality, integrity, and availability**—including the systems and hardware that use, store, and transmit that information.

🔷 **Components of Information Security**

InfoSec is maintained through:

- **Policies** – Define rules and procedures.
- **Training and Awareness Programs** – Educate employees about risks and best practices.
- **Technology** – Provides technical protection (e.g., firewalls, encryption).

🔷 **Areas Covered by Information Security**

- **Information Security Management**
- **Computer and Data Security**
- **Network Security**
- These areas **overlap through policy**, which connects and guides them.

🧊 CNSS Security Model (McCumber Cube)

🔷 Overview

- **Developed by:** John McCumber.
- **Document Source:** CNSS (Committee on National Security Systems), **NSTISSI No. 4011 – National Training Standard for Information Security Professionals.**
- **Purpose:** Provides a **comprehensive model** for understanding and implementing **information security**.
- **Also Known As:** The **McCumber Cube**.
- **Structure:** A **3 × 3 × 3 cube (27 cells)** that represents all areas that must be addressed in securing information systems.

🔷 Three Dimensions of the CNSS Model

The model has **three axes (dimensions)**, each containing **three components**:

1. Information States (Where data exists)

- **Storage** – Data at rest (saved on devices or media).
- **Processing** – Data being actively used or modified.
- **Transmission** – Data being sent across networks or between devices.

2. Security Goals (Information protection principles)

- **Confidentiality** – Ensuring that information is accessible only to authorized individuals.
- **Integrity** – Maintaining accuracy, consistency, and trustworthiness of data.
- **Availability** – Ensuring information and systems are accessible when needed.

3. Security Measures (How protection is achieved)

- **Policy and Procedures** – Rules, guidelines, and management controls.
- **Education, Training, and Awareness (ETA)** – Ensuring people understand and apply security principles.
- **Technology** – Technical controls like firewalls, encryption, intrusion detection systems, etc.

🔷 How the Model Works

- The cube's **27 cells (3×3×3)** represent **intersections** between:
  - The **security goals**,
  - The **information states**, and
  - The **security measures**.
- Each intersection (cell) identifies a **specific area that must be addressed** to secure information.
  - Example: The intersection of **Technology + Integrity + Storage** could involve a **Host Intrusion Detection System (HIDS)** that alerts administrators when a critical file is modified.

🔷 Purpose and Benefits

- Helps **design or review** an organization's information security program.
- Ensures **complete coverage** by addressing all areas of security.
- **Identifies gaps** in existing security measures.