I. Core Concepts

- **Information System (IS) Components**: An IS includes software, hardware, data, people, procedures, and networks.
    - **Software**: Often the **most difficult to secure** and a frequent target of attack.
    - **Hardware**: Requires physical security policies to secure physical locations, laptops, and flash memory.
    - **Data**: Frequently the **most valuable asset** and the main target of attacks.
    - **Procedures**: Can pose a threat to the integrity of data.
    - **People**: ***Considered the weakest link*** and are prone to social engineering. They require training and awareness.
    - **Networks**: Require different security measures than physical spaces.
- **Security Mindset**: A crucial aspect of information assurance.
- **Risk Management**: A key focus that involves quantifying risks, understanding the difference between threats and vulnerabilities, and assessing business impact.
- **Detection and Response Controls**: Essential for managing security incidents.
- **Computer as Subject and Object of Attack**: A computer can be the tool used to carry out an attack or the target of an attack.
    - **Direct Attack**: A hacker uses their computer to break into a system.
    - **Indirect Attack**: A compromised system is used to attack other systems.
- **Balancing Security and Access**: Security should balance protection and availability, allowing reasonable access while guarding against threats. **100% security is impossible to achieve; it is a process, not an absolute certainty.**

II. Approaches to Information Security Implementation

- **Bottom-Up Approach**:
    - A grassroots effort where system administrators improve security.
    - Advantage: Utilizes the technical expertise of individual administrators.
    - Disadvantages: Often lacks participant support and organizational staying power, which can lead to inconsistent security measures and a fragmented risk management strategy.

- **Top-Down Approach**:
    - Initiated by upper management with policies, procedures and processes.
    - Goals and outcomes are dictated, and accountability is determined.
    - Most effective when combined with a formal development strategy like the Systems Development Life Cycle (SDLC).

III. Systems Development Life Cycle (SDLC)

- **SDLC**: A methodology for implementing information systems [6].
- Ensures a rigorous process and avoids missing steps [7].
- Aids in creating a comprehensive security posture [7].
- Traditional SDLC phases can be adapted to support specialized implementation of IS projects.
- **Security SDLC**: A coherent program to identify threats and create countermeasures, rather than a series of disconnected actions.
- **Investigation**: Defines process, outcomes, goals, and constraints based on enterprise information security policy [8].
- **Analysis**: Examines existing security policies and legal issues and performs risk analysis [8].
- **Logical Design**: Creates security blueprints, incident response actions, and performs feasibility analysis [8].
- **Physical Design**: Evaluates and selects security technology.
- **Implementation**: Acquires, tests, and implements security solutions, including personnel training.
- **Maintenance and Change**: Involves constant monitoring, testing, and updating due to changing threats.

IV. Key Stakeholders

- **Security Professionals and the Organization**: A wide range of professionals are needed to support security programs [10].
- **Senior Management**: Plays a vital role, including the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).
- **CIO**: Advises senior executives on strategic planning.

- **CISO**: Responsible for assessing, managing, and implementing IS, reporting to the CIO [11].
- **Information Security Project Team**: Includes a champion, team leader, security policy developers, risk assessment specialists, security professionals, systems administrators, and end users [11, 12].
- **Data Ownership**:
- **Data Owner**: Responsible for security and use of information [12].
- **Data Custodian**: Responsible for storage, maintenance, and protection of information [12].
- **Data Users**: End users who work with information [12].
- **Communities of Interest**: Groups of individuals united by similar interests or values within an organization, such as information security, IT, and organizational management professionals [12, 13].

V. Information Assurance (IA) Analysis Model

- **McCumber Cube**: A model framework for establishing and evaluating information security programs.
  - The model is based on four dimensions: **Information States, Security Services, Security Countermeasures, & Time**.
    - **Information States**: Information can be stored, processed, or transmitted.
    - **Security Services**: Include availability, integrity, confidentiality, authentication, and non-repudiation.
    - **Security Countermeasures**: Safeguard systems via technology, operations, and people. People require training and education.
    - **Time**: Data accessibility can be online or offline, and information systems are constantly in flux.
- **Understanding IAS**: Requires understanding the interaction of model components rather than individual components.
- **Reference Model for IAS**: Provides a visual representation for organizing domain knowledge.

VI. Information Value and Threat Analysis

- **Information Value**: The value of information depends on its use, purpose, and context.
  - It is the weight of significance and importance of a particular information on the perspective of the information user.

- **Threat Analysis**: A process to determine which system components need protection and the types of threats they face.
    - Closely related to risk assessment.
    - Involves identifying threats and vulnerabilities.
- **Types of Threats**: Natural, human, and political. Only probable threats should be considered.
- **Threat Categories**: By intent (accidental or purposeful), entity (human, processing, natural) and impact (type of asset, consequences).
- **Impacts of Threats**: Interruption, interception, modification, and fabrication.
- **Steps in Threat Analysis**
    1. determine information value
    2. identify and prioritize assets
    3. identify threats
    4. identify vulnerabilities
    5. analyze controls
    6. determine likelihood of incidents
    7. assess impact
    8. prioritize security risks
- **Threat Modeling**: Creates an abstraction of the system, profiles of potential attackers, and a catalog of potential threats.
    - **STRIDE**: A **mature** threat-modeling method

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Table 1: STRIDE Threat Categories

        - Developed by Microsoft.
    - **PASTA**: A **risk-centric** threat-modeling framework.
        - Process for Attack Simulation and Threat Analysis
    - **LINDDUN**: Focuses on **privacy** concerns and data security.

    - linkability, identifiability, nonrepudiation, detectability, disclosure of
    - information, unawareness, noncompliance)
  - **Attack Trees**: Diagrams that depict attacks on a system in a tree form.

VII. Disaster Recovery

- **Disaster**: An event causing significant disruption in operational and/or computer processing capabilities.
- **Types of Disasters**: Natural/environmental, technical/mechanical, and human activities/threats.
- **Disaster Recovery (DR)**: Aims to protect an organization from the effects of significant negative events. It is a method of regaining access and functionality to IT infrastructure after disasters.
  - Involves policies, tools, and procedures for recovering vital technology infrastructure.
- **Disaster Recovery Plan (DRP)**: A documented approach for quickly resuming work after an unplanned incident, ensuring the continuation of vital business processes.
  - Designed to restore data and critical applications.
- **Disaster recovery is a subset of business continuity planning**.
- **Disaster Recovery Management System**: An ongoing process of planning, developing, testing, and implementing DR procedures.
  - Key elements include Critical Application Assessment, Back-Up Procedures, Recovery Procedures, Implementation Procedures, Test Procedures, and Plan Maintenance.
- **Disaster Recovery Strategy**: Involves relocating critical Information Systems processing to an alternate computer-processing center, often at a hot-site.
- **Disaster Recovery Phases**: Prevention, preparedness, response, and recovery.
  - **Prevention**: Involves minimizing risks and establishing routine maintenance measures.
  - **Preparedness**: Includes developing a written plan, training a response team, and keeping documentation up to date.
  - **Response**: Follows emergency procedures for evacuation and assesses damage.
  - **Recovery**: Restores critical applications and data from backup.

VIII. Cryptology and Cryptography

- **Cryptology**: The **science of hiding**, encompassing both cryptography and cryptanalysis.
- **Cryptanalysis**: The **science of recovering** secured information without knowledge of the key. It is essentially ***breaking codes.***
- **Cryptography**: The art of secret writing. It is the method of protecting information via codes, so only intended users can read it.
    - Involves transformation and secrets.
- **Encryption**: A process that encodes a message so it can only be read by certain people. It is the process of turning text into code.
- **Decryption**: The conversion of encrypted data into its original form.
- **Cipher**: A secret or disguised way of writing a message. It is an algorithm for encryption or decryption.
    - Classical ciphers include substitution and transposition ciphers.
        - **Caesar Cipher**: A type of substitution cipher where each letter is shifted a number of places down the alphabet.
        - **Substitution Cipher**: Replaces plaintext units with ciphertext based on a fixed system.
        - **Atbash Cipher**: A substitution cipher that reverses the alphabet.
        - **Transposition Cipher**: Shifts the positions of plaintext units to create ciphertext.
        - **Rail Fence Cipher**: A transposition cipher where plaintext is written diagonally on rails, then read off in rows.
        - **Scytale Cipher**: A mechanical transposition cipher used by ancient Greeks.
        - **Shift Key Cipher**: Encrypts by shifting each letter of the plaintext by n positions. The Caesar cipher is a type of shift key cipher.

IX. Modern Cryptography

- **Block Cipher**: Encrypts blocks of text using a symmetric key and deterministic algorithm.
    - Encrypts chunks of data
    - Better for large amounts of data
- **Stream Cipher**: Combines plaintext digits with a pseudorandom cipher digit stream.
    - Encrypts one bit at a time

- Best suited for real time applications
- **Cryptosystem**: A suite of cryptographic algorithms for a particular security service.
- **Cryptographic Algorithms**: Grouped into symmetric and asymmetric.
- **2 main types of Encryption**
    - **Symmetric-Key Encryption**: **Uses one shared key for both encryption and decryption**. It is speedy, efficient, and good for storing documents, but the key must be kept secret.
        - *Examples include Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES).*
    - **Asymmetric-Key Encryption**: **Uses two different but related keys**, where one key encrypts and the other decrypts. It is also known as public-key encryption. Processing time is higher, but it offers a high level of security.
        - Public key and private key
- **Diffie-Hellman Key Exchange**: **Allows two parties to establish a shared secret key** over an insecure channel.

X. Public Key Infrastructure (PKI) and Planning

- **Public Key Infrastructure (PKI)**: Procedures and infrastructure to store, issue, revoke certificates, and manage public keys.
    - It also facilitates secure electronic transfers of information.
    - PKI is required for activities where passwords are not sufficient authentication.
    - **Digital Certificate**: An electronic "password" for secure data exchange using PKI.
    - *The **Philippine National Public Key Infrastructure (PNPKI)** is an initiative of the **Department of Information and Communications Technology (DICT)***
- **IT Security Planning**: Essential because 100% security is impossible.
    - Involves inventory of assets (devices, online accounts, etc.)
    - risk assessment
    - SWOT analysis
    - development of a security plan
- **Cybersecurity**: Protects internet-connected systems from cyber threats and deals with cybercrimes and law enforcement. It is a practice used to protect against unauthorized access to data centers and systems.

- **IT Security Architecture**: Positions security controls and breach countermeasures in relation to a company's overall system.
    - **Security Education, Training, and Awareness (SETA)**: Reduces security breaches due to lack of employee awareness. It sets the security tone and explains the employees' role in security.
        - Training people / raising awareness
        - Building a human firewall
        - Technology alone cannot solve issues controlled by individuals.
- **Continuity Strategies**: Include preventive (mitigation), crisis response, and recovery strategies.
- Companies may divide business continuity planning into planning and prevention, disaster response, and return to normal.
    - Occupant Emergency Plan (OEP),
    - Incident Response Plan (IR Plan),
    - Continuity of Operations Plan (COOP),
    - Disaster Recovery Plan (DR Plan),
    - Continuity of Support Plan (CS Plan) and
    - Business Resumption Plan (BRP).