IT311 – Information Assurance Security

MIDTERM REVIEWER EXAM

Introduction to Information Security (Chapter 1)

- **Information Security: Protection of information and its critical elements, including systems and hardware that store, use, and transmit that information.**
- **Confidentiality: Ensuring that information is accessible only to authorized users.**
- **Integrity: Maintaining the accuracy and completeness of data.**
- **Availability: Ensuring that information is accessible when needed by authorized users.**
- **Authenticity: Verifying that users are who they claim to be and that data comes from trusted sources.**
- **Non-repudiation: Assurance that someone cannot deny the validity of their actions regarding data or transactions.**

Components of Information Systems:

- **Software: Programs that process data.**
- **Hardware: Physical devices used in data processing.**
- **Data: Information requiring protection.**
- **People: Users and personnel interacting with the system.**
- **Procedures: Policies and processes governing system use.**
- **Networks: Systems for transmitting data.**

Security Systems Development Life Cycle (SecSDLC): A framework to integrate security into the system development process.

2. The Need for Security (Chapter 2)

Organizational Functionality: Importance of security in maintaining an organization's ability to operate effectively.
Safe Operations: Ensuring that applications and processes run securely.

Protecting Data: **Preventing unauthorized access** or data loss.
Safeguarding Technology: Protecting hardware and software assets.

Common Threats:

- **Intellectual Property Compromises**: Unauthorized access to proprietary information.
- **Software Attacks**: Deliberate attacks like malware.
- **Human Error**: Mistakes leading to security breaches.
- **Natural Disasters**: Events causing data loss or system damage.
- **Technical Failures**: Hardware or software malfunctions.

Types of Attacks:

- **Malicious Code**: Includes viruses, worms, and ransomware.
- **Spoofing**: Impersonating legitimate users or systems.
- **Denial of Service (DoS)**: Making a system unavailable to users.
- **Social Engineering**: Manipulating individuals into revealing confidential information.

- **Threats**: Covers common threats, including intellectual property compromises, software attacks, human error, natural disasters, and technical failures.
- **Attacks**: Discusses methods such as malicious code, spoofing, DoS attacks, and social engineering.

3. Legal, Ethical, and Professional Issues (Chapter 3)

Legal Regulations: Laws governing information security practices, including privacy and data protection laws.
Ethical Considerations: Challenges and responsibilities in maintaining ethical standards in security practices.

Codes of Ethics: **Guidelines for ethical behavior** in information security, as established by organizations like ACM and ISC².

Ten Commandments of Computer Ethics: Fundamental ethical principles guiding behavior in computer and information security contexts.

Risk Management (Chapter 4)

Risk Management: **Process** of identifying, assessing, and controlling risks to information assets.
Risk Identification: **Recognizing** potential threats and vulnerabilities.
Risk Assessment: **Evaluating** the likelihood and impact of risks.
Risk Control Strategies:

- **Defend**: **Implementing measures** to prevent risks.
- **Transfer**: **Shifting the risk** to a third party (e.g., insurance).
- **Mitigate**: **Reducing the impact** or likelihood of risks.
- **Accept**: **Acknowledging the risk** without taking action.
- **Terminate**: **Eliminating** the risk by discontinuing the activity.

Cost-Benefit Analysis: **Evaluating the financial implications of** risk management strategies to determine the most effective approach.