CISSP Domain 1: Security and Risk Management

Business Continuity and Disaster Recovery

- Planning and Preparation
  - Business continuity planning ensures critical functions can continue during a crisis.
  - Disaster recovery focuses on restoring IT systems and data after an incident.
- Testing and Maintenance of Plans
  - Regular testing of business continuity and disaster recovery plans is essential for effectiveness.
  - Continuous improvement based on test outcomes helps adapt to new challenges.

Security Awareness Training

- Importance of Training Programs
  - Security awareness training educates employees about potential threats and best practices.
  - Helps to create a culture of security within the organization.
- Training Implementation Strategies
  - Use various formats such as workshops, e-learning, and simulations to engage employees.
  - Regularly update training content to reflect current threats and trends.

Security Policies and Procedures

- Development of Security Policies
  - Security policies define the organization's approach to protecting its information assets.
  - They establish the rules and guidelines for employees and stakeholders.
- Implementation and Enforcement
  - Procedures for policy enforcement include training and monitoring compliance.
  - Regular audits ensure that policies are adhered to and remain effective.

Basic Principles

- Overview of Security and Risk Management
  - Security and risk management address the protection of information assets.
  - It includes the identification of risks and the implementation of controls to mitigate them.
- Key Concepts of Confidentiality, Integrity, and Availability
  - Confidentiality ensures that information is accessible only to authorized users.
  - Integrity protects information from unauthorized modification.
  - Availability guarantees that information and resources are accessible when needed.

Governance, Risk, and Compliance

- Frameworks and Standards
  - Various frameworks like ISO/IEC 27001 provide guidelines for managing information security.
  - Compliance requirements such as GDPR define the legal standards for data protection.
- Risk Management Process
  - Identify assets, threats, and vulnerabilities to assess risks.
  - Implement risk mitigation strategies and regularly review their effectiveness.