Certified Information Systems Security Professional (CISSP)

1. **Security and Risk Management**
    a. Understand and apply concepts of confidentiality, integrity and availability
    b. Evaluate and apply security governance principles
    c. Determine compliance requirements
    d. Understand legal and regulatory issues that pertain to information security in a global
    e. Understand, adhere to, and promote professional ethics
    f. Develop, document, and implement security policy, standards, procedures, and guidelines
    g. Identify, analyze, and prioritize Business Continuity (BC) requirements
    h. Contribute to and enforce personnel security policies and procedures
    i. Understand and apply risk management concepts
    j. Understand and apply threat modeling concepts and methodologies
    k. Apply risk-based management concepts to the supply chain
    l. Establish and maintain a security awareness, education, and training program
2. **Asset Security**

. Identify and classify information and assets
    a. Determine and maintain information and asset ownership
    b. Protect privacy
    c. Ensure appropriate asset retention
    d. Determine data security controls
    e. Establish information and asset handling requirements

3. **Security Architecture and Engineering**

. Implement and manage engineering processes using secure design principles
    a. Understand the fundamental concepts of security models
    b. Select controls based upon systems security requirements
    c. Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
    d. Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
    e. Assess and mitigate vulnerabilities in web-based systems
    f. Assess and mitigate vulnerabilities in mobile systems
    g. Assess and mitigate vulnerabilities in embedded devices
    h. Apply cryptography
    i. Apply security principles to site and facility design
    j. Implement site and facility security controls

4. **Communication and Network Security**

. Implement secure design principles in network architectures

   a. Secure network components

   b. Implement secure communication channels according to design

5. **Identity and Access Management (IAM)**

. Control physical and logical access to assets

   a. Manage identification and authentication of people, devices, and services

   b. Integrate identity as a third-party service

   c. Implement and manage authorization mechanisms

   d. Manage the identity and access provisioning lifecycle

6. **Security Assessment and Testing**

. Design and validate assessment, test, and audit strategies

   a. Conduct security control testing

   b. Collect security process data (e.g., technical and administrative)

   c. Analyze test output and generate report

   d. Conduct or facilitate security audits

7. **Security Operations**

. Understand and support investigations

   a. Understand requirements for investigation types

   b. Conduct logging and monitoring activities

   c. Securely provisioning resources

   d. Understand and apply foundational security operations concepts

   e. Apply resource protection techniques

   f. Conduct incident management

   g. Operate and maintain detective and preventative measures

   h. Implement and support patch and vulnerability management

   i. Understand and participate in change management processes

   j. Implement recovery strategies

   k. Implement Disaster Recovery (DR) processes

   l. Test Disaster Recovery Plans (DRP)

   m. Participate in Business Continuity (BC) planning and exercises

   n. Implement and manage physical security

   o. Address personnel safety and security concerns

8. **Software Development Security**

. Understand and integrate security in the Software Development Life Cycle (SDLC)

   a. Identify and apply security controls in development environments

   b. Assess the effectiveness of software security

   c. Assess security impact of acquired software

   d. Define and apply secure coding guidelines and standards