



Certified Information Systems Security Professional (CISSP)

Course Details

Course Outline

1. Security and Risk Management

- Understand and apply concepts of confidentiality, integrity and availability
- Evaluate and apply security governance principles
- Determine compliance requirements
- Understand legal and regulatory issues that pertain to information security in a global
- Understand, adhere to, and promote professional ethics
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modeling concepts and methodologies
- Apply risk-based management concepts to the supply chain
- Establish and maintain a security awareness, education, and training program

2. Asset Security

- Identify and classify information and assets
- Determine and maintain information and asset ownership
- Protect privacy
- Ensure appropriate asset retention
- Determine data security controls
- Establish information and asset handling requirements

3. Security Architecture and Engineering

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models



- Select controls based upon systems security requirements
- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Assess and mitigate vulnerabilities in web-based systems
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices
- Apply cryptography
- Apply security principles to site and facility design
- Implement site and facility security controls

4. Communication and Network Security

- Implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

5. Identity and Access Management (IAM)

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Integrate identity as a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle

6. Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate report
- Conduct or facilitate security audits

7. Security Operations

- Understand and support investigations
- Understand requirements for investigation types



- Conduct logging and monitoring activities
- Securely provisioning resources
- Understand and apply foundational security operations concepts
- Apply resource protection techniques
- Conduct incident management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

8. Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure coding guidelines and standards