(ISC)² CISSP Certification

Certified Information Systems Security Professional

Domain 1: Security and Risk Management

- Understand, adhere to, and promote professional ethics

- Understand and apply security concepts

- Evaluate and apply security governance principles

- Determine compliance and other requirements

- Understand legal and regulatory issues that pertain to information security in a holistic context

- Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

- 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 Supply Chain Risk Management (SCRM) concepts

- Establish and maintain a security awareness, education, and training program

Domain 2: Asset Security

- Identify and classify information and assets

- Establish information and asset handling requirements

- Provision resources securely

- Manage data lifecycle

- Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

- Determine data security controls and compliance requirements

Domain 3: Security Architecture and Engineering

- Research, implement and manage engineering processes using secure design principles

- Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

- Select controls based upon systems security requirements

- Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Select and determine cryptographic solutions

- Understand methods of cryptanalytic attacks

- Apply security principles to site and facility design

- Design site and facility security controls

Domain 4: Communication and Network Security

- Assess and implement secure design principles in network architectures

- Secure network components

- Implement secure communication channels according to design

Domain 5: Identity and Access Management (IAM)

- Control physical and logical access to assets

- Manage identification and authentication of people, devices, and services

- Federated identity with a third-party service

- Implement and manage authorization mechanisms

- Manage the identity and access provisioning lifecycle

- Implement authentication systems

Domain 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

Domain 7: Security Operations

- Understand and comply with investigations

- Conduct logging and monitoring activities

- Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)

- Apply foundational security operations concepts

- Apply resource protection

- 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

Domain 8: Software Development Security

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

- Identify and apply security controls in software development ecosystems

- Assess the effectiveness of software security

- Assess security impact of acquired software

- Define and apply secure coding guidelines and standards