CISSP Exam Prep Training - Course Content

Domain 1 Security and Risk Management (16%)

1.1 Understand, adhere to, and promote professional ethics

1.2 Understand and apply security concepts

1.3 Evaluate and apply security governance principles

1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context

1.5 Understand requirements for investigation types

1.6 Develop, document, and implement security policy, standards, procedures, and guidelines

1.7 Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements

1.8 Contribute to and enforce personnel security policies and procedures

1.9 Understand and apply risk management concepts

1.10 Understand and apply threat modeling concepts and methodologies

1.11 Apply Supply Chain Risk Management (SCRM) concepts

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

Domain 2 Asset Security (10%)

2.1 Identify and classify information and assets

2.2 Establish information and asset handling requirements

2.3 Provision information and assets securely

2.4 Manage data lifecycle

2.5 Ensure appropriate asset retention

2.6 Determine data security controls and compliance requirements

Domain 3 Security Architecture and Engineering (13%)

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

3.2 Understand the fundamental concepts of security models

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of Information Systems

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

3.6 Select and determine cryptographic solutions

3.7 Understand methods of cryptanalytic attacks

3.8 Apply security principles to site and facility design

3.9 Design site and facility security controls

3.10 Manage the information system lifecycle

Domain 4 Communication and Network Security (13%)

4.1 Apply secure design principles in network architectures

4.2 Secure network components

4.3 Implement secure communication channels

Domain 5 Identity and Access Management (IAM) (13%)

5.1 Control physical and logical access to assets

5.2 Design identification and authentication strategy

5.3 Implement federated identity

5.4 Implement and manage authorization mechanisms

5.5 Manage the identity and access provisioning lifecycle

5.6 Implement authentication systems

Domain 6 Security Assessment and Testing (12%)

6.1 Design and validate assessment, test, and audit strategies

6.2 Conduct security control testing

6.3 Collect security process data

6.4 Analyze test output and generate report

6.5 Conduct or facilitate security audits

Domain 7 Security Operations (13%)

7.1 Understand and comply with investigations

7.2 Conduct logging and monitoring activities

7.3 Perform configuration management

7.4 Apply foundational security operations concepts

7.5 Apply resource protection

7.6 Conduct incident management

7.7 Operate and maintain detection and preventative measures

7.8 Implement and support patch and vulnerability management

7.9 Understand and participate in change management processes

7.10 Implement recovery strategies

7.11 Implement Disaster Recovery processes

7.12 Test Disaster Recovery Plans

7.13 Participate in Business Continuity planning

7.14 Implement and manage physical security

7.15 Address personnel safety and security concerns

Domain 8 Software Development Security (10%)

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

8.2 Identify and apply security controls in software development ecosystems

8.3 Assess the effectiveness of software security

8.4 Assess security impact of acquired software

8.5 Define and apply secure coding guidelines and standards