Certified Information Systems Security Professional - Eng.

Duration: 5 Days

COURSE DESCRIPTION

The CISSP Exam Preparation course is an intensive, five-day examination preparation program to prepare individuals who are planning to sit for the Certified in Information Systems Security Professional (CISSP) exam.

The course focuses on the security domains covered in the 2021 Common Body of Knowledge and includes class lectures, group discussions/activities, exam practice and answer debriefs. The course is intended for individuals with familiarity with and experience in the field of information security

LEARNING OBJECTIVES:

Participants in the CISSP Exam Preparation course will be provided instruction designed to provide the following:

- An understanding of the format and structure of the CISSP certification exam.
- A knowledge of the various topics and technical areas covered by the exam.
- Practice with specific strategies, tips and techniques for taking and passing the exam
- Opportunities to execute practice questions with debriefs of answers

COURSE OUTLINE

1.Introduction

- Who Should Take This Course?
- About (ISC)2
- CISSP Certification
- CISSP Examination
- CBK Review, Domain and Function Areas

2. Security &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 security awareness, education, and training program

3. Asset Security

- Identify and classify information and assets
- Establish information and asset handling requirements
- Provision resources securely
- Manage data lifecycle
- Ensure appropriate asset retention
- Determine data security controls and compliance requirements

4. Security Architecture and Engineering

- Research, 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 (IS)
- 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 Identify and classify information and assets

5. Communication & Network Security

- Assess and implement secure design principles in network architectures
- Secure network components.
- Implement secure communication channels according to design

6. Identity & Access Management

- 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 life cycle
- Implement authentication systems

7. Security Assessment & 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

8. Security Operations

- Understand and comply with investigations
- Conduct logging and monitoring activities
- Perform Configuration Management 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

9.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

WHO SHOULD ATTEND

The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles

PREREQUISITES

There are no prerequisite requirements for taking the CISSP Exam Preparation Course or the CISSP exam; however, in order to apply for CISSP certification, the candidate must meet the necessary experience requirements determined by ISC2.

ASSESSMENT

- 40 Multiple Choice Questions
- 1 hour duration
- Closed book
- 60% to pass

ISC EXAMINATION FORMAT (optional / not included)

- Computerized Adaptive Testing
- Multiple Choice and Advanced Innovative Questions
- Up to 150 questions 3 hours duration
- Maximum Possible Score of 1000 points 700 points required to pass

CERTIFICATION

Delegates who successfully completed the course and pass the exam will be allowed to apply for formal CISSP accreditation from ISC

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th