Certified Information Systems Security Professional (CISSP)

Duration 5 Days

COURSE CONTENT

The CISSP has clearly emerged as THE key certification for security professionals. In fact, in an informal survey of information security jobs on a major employment Web site, over 70 percent of the positions required CISSP certification! Corporations are demanding experienced information security professionals with the certifications to prove it to protect their information and assets.

In line with the revision of the CISSP Body of Knowledge by ISC2 in April 2015, our course has been prepared with great care to provide the most exhaustive survey of the CISSP information, test taking techniques, and preparation materials available in the industry. While other CISSP courses on the market require extensive reading and practice test preparation between finishing the class and taking the exam, our students have consistently found that the high quality of our course and its in-class practice test result in a minimum of extra time spent preparing for a successful pass of the exam. In today's hectic business conditions, time is of the essence!

COURSE OBJECTIVES

The CISSP Prep class was developed to meet current demands and the growing needs of the computer industry. This class provides the student with the level of knowledge needed as part of the (ISC)2 certification requirements for the Certified Information System Security Professional (CISSP) Certification. This certification is rapidly becoming a requirement for employment with security tasks. Students gain a solid background on security concerns, communications, infrastructure, basic cryptography, and operational

WHO NEEDS TO ATTEND

CISSP certification is beneficial to IT consultants, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

EXAMINATION

- Computer Adaptive Testing (CAT) - English Exam
- 3 Hours
- 100 - 150 questions
- Multiple choice and advanced innovative questions
- A passing score is 700 out of 1000 points

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

COURSE CONTENT

1. Introduction

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

2. Security & Risk Management

- Confidentiality, Integrity & Availability
- Security Governance – Alignment of security function to strategy, goals, mission and objectives; organizational processes; security roles and responsibilities; due care and due diligence
- Compliance – Legislative and regulatory; privacy requirements compliance
- Legal & Regulatory Issues Pertaining to Information Security in Global Context – Computer Crimes; Licensing and intellectual property; import/export controls; trans-border data flow; privacy; data breaches
- Professional Ethics
- Documented Security Policy, Standards, Procedures & Guidelines
- Business Continuity Requirements
- Personnel Security Policies
- Risk Management Concepts
- Threat Modeling – identifying; determining and diagramming potential attacks; reduction analysis; technologies and processes to remediate threats
- Security Risk Considerations Integrated into Acquisition Strategy & Practice – hardware, software and services; third-party assessment and monitoring; minimum security requirements and service-level requirements
- Information Security Education, Training & Awareness

3. Asset Security

- Classify Information and Supporting Assets
- Determine & Maintain Ownership
- Data Privacy
- Retention
- Data Security Controls
- Handling Requirements

4. Security Engineering

- Engineering Processes Using Secure Design Principles
- Concepts of Security Models
- Controls & Countermeasures
- Security Capabilities of Information Systems
- Assess & Mitigate Vulnerabilities of Security Architectures, Designs & Solution Elements – client-based; server-based; database security; large-scale parallel systems; distributed systems; cryptographic systems; industrial control systems
- Assess & Mitigate Vulnerabilities in Web-based Systems
- Assess & Mitigate Vulnerabilities in Mobile Systems
- Assess & Mitigate Vulnerabilities in in Embedded Devices & Cyber-Physical Systems
- Apply Cryptography – life cycle; types; PKI; key management practices; digital signatures; digital rights management; non-repudiation; integrity; methods of cryptanalytic attacks
- Secure Principles: Site and Facility Design

- Design & Implement Physical Security

5. Communication & Network Security

- Secure Design Principles Applied to Network Architecture – OSI and TCP/IP models; IP networking; implications of multilayer protocols; converged protocols; software-defined networks; wireless networks; cryptography used to maintain communication security
- Secure Network Components – operation of hardware; transmission media; network access control devices; endpoint security; content-distribution networks; physical devices
- Secure Communication Channels – voice; multimedia collaboration; remotes access; data communications; virtualized networks
- Prevent or Mitigate Network Attacks

6. Identity & Access Management

- Control Physical & Logical Access to Assets
- Manage Identification & Authentication of People and Devices
- Identity as a Service
- Third-Party identity Services
- Implement & Manage Authorization Mechanisms
- Prevent or Mitigate Access Controls Attacks
- Manage Identity & Access Provisioning Lifecycle

7. Security Assessment & Testing

- Design & Validate Assessment & Test Strategies
- Conduct Security Control Testing.
- Collect Security Process Data
- Analyze & Report Test Outputs
- Conduct or Facilitate Internal & Third Party Audits

8. Security Operations

- Investigations – evidence collection and handling; reporting and documenting; investigative techniques; digital forensics
- Requirements for Investigation Types – operations; criminal; civil; regulatory; eDiscovery
- Logging & Monitoring Activities
- Sure Provisioning of Resources
- Foundational Security Operations Concepts
- Resource protection Techniques
- Incident Management
- Operate & Maintain Preventative Measures
- Patch & Vulnerability Management
- Change Management Processes
- Recovery Stages – backup storage strategies; recovery site strategies; multiple processing sites; system resilience, high availability, quality of service and fault tolerance
- Disaster Recovery Processes
- Test Disaster Recovery Plans
- Business Continuity Planning & Exercises
- Implement & Manage Physical Security
- Address Personal Safety Concerns

9. Software Development Security

- Security in the Software Development Lifecycle
- Security Controls in Development Environments
- Assess Effectiveness of Software Security
- Assess Security Impact of Acquired Software