CISSP Preparation

Course Summary

Description

This intensive training course in designed for individuals who are getting prepared to become CISSP certified. In this class, you will be hearing 3.5-4 hour lectures from subject matter experts (SMEs) on each of the ten domains in the Common Body of Knowledge covered in the CISSP exam.

Objectives
At the end of this course, students will be able to:

- Gauge their ability to pass the CISSP exam and complete the training with a customized, focused plan to identify and reinforce their areas of weakness, and to successfully master the rigorous CISSP examination.

Topics

- Security Management Domain
- Business Continuity Planning and Disaster Recovery Planning Domain
- Law, Investigations & Ethics Domain
- Operations Security Domain
- Physical Security Domain
- Access Control Systems
- Applications and Systems Development Security Domain
- Cryptography Domain
- Security Architecture and Models Domain

Audience

This course is designed for the information security practitioner who is looking to achieve professional certification as a CISSP (Certified Information Systems Security Professional).

Prerequisites

Students should have a minimum of three years in the information security field.

Duration

Five days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

CISSP Preparation

Course Outline

I. Security Management Domain
- A. Change Control/Management
- B. Data Classification
- C. Employment Policies and Practices
- D. Policies, Standards, Guidelines and Procedures
- E. Risk Management Tools and Methodologies
- F. Security Roles and Responsibilities
- G. Security Awareness Training
- H. Security Management Planning

II. Business Continuity Planning and Disaster Recovery Planning Domain
- A. Business Continuity Project Scoping and Planning
- B. Business Impact Assessment
- C. Recovery Strategy Determination
- D. Recovery Plan Development
- E. Recovery Plan Implementation
- F. Restoration

III. Law, Investigations & Ethics Domain
- A. Computer Laws
- B. Computer Crime
- C. Evidence Identification, Collection and Preservation
- D. Incident Handling
- E. Investigative Processes and Techniques
- F. Computer Ethics

IV. Operations Security Domain
- A. Administrative Management
- B. Anti-Virus Management
- C. Critical Information Backup
- D. Workstations/Location Changes
- E. Need-to-Know/Least Privilege
- F. Record Retention
- G. Sensitive Information/Media Security
- H. Resource Protection
- I. Type of Attacks
- J. Violations, Breaches and Reporting

V. Physical Security Domain
- A. Physical Security Threats
- B. Site Design and Configurations
- C. Technical Controls
- D. Environmental and Life Safety Controls

VI. Access Control Systems
- A. Types of Access Control
- B. Administering Access Control
- C. Access Control Techniques
- D. Access Rights and Permissions
- E. Rule of Least Privilege
- F. Accountability
- G. Identification and Authentication Techniques
- H. Centralized Access Control
- I. Decentralized Access Control
- J. File and Data Ownership and Custodianship
- K. Attack Methods
- L. Penetration Testing
- M. Monitoring
- N. One-Time Passwords
- O. Password Controls
- P. Single Sign-On

VII. Applications and Systems Development Security Domain
- A. Application Controls
- B. Attacks
- C. Databases
- D. Data Warehousing
- E. Knowledge-Based Systems
- F. Systems Development Controls

VIII. Cryptography Domain
- A. Authentication
- B. Encryption
- C. Error Detection/Correction Features
- D. Hash Functions
- E. Message Digests
- F. Kerberos
- G. Certificate Authority
- H. One-Time Cipher Keys
- I. Private Key Algorithms
- J. Public Key Algorithms

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

CISSP Preparation

Course Outline (cont'd)

K. Digital Signatures and Non-Repudiation
L. Key Escrow
M. Stream Ciphers

IX. Security Architecture and Models Domain

A. Principles of Common Computer and Network Organizations, Architectures and Designs
B. Principles of Common Security Models, Architectures and Evaluation Criteria
C. Common System Architectures and Design Flaws and Security Issues

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically