ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Certified Information Systems Security Professional-CISSP

Course Summary

Description

CISSP® is the global benchmark for information security professionals. It is a highly sought after certification for those people who are looking to make a career in Information Security.

This globally recognized credential validates your technical knowledge and understanding of information security issues - and proves you have what it takes to protect your organization.

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

- Security and Risk Management (Security, Risk, Compliance, Law, Regulations, Business Continuity)
- Asset Security (Protecting Security of Assets)
- Security Engineering (Engineering and Management of Security)
- Communications and Network Security (Designing and Protecting Network Security)
- Identity and Access Management (Controlling Access and Managing Identity)
- Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
- Security Operations (Foundational Concepts, Investigations, Incident Management, Disaster Recovery)
- Software Development Security (Understanding, Applying, and Enforcing Software Security)

Topics

- Access Control Systems & Methodologies
- Telecommunications & Network Security
- Security Management Practices
- Applications & systems Development Security
- Cryptography
- Alternatives (e.g., steganography and watermarking)
- Security Architecture Models
- Operations Security
- Business Continuity & Disaster Planning
- Law, Investigations, and Forensics & Ethics

Audience

This course is designed for information security professionals.

Prerequisites

There are no prerequisites for this course.

Duration

Four 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!"

Certified Information Systems Security Professional-CISSP

Course Outline

I. Access Control Systems & Methodologies
- A. Control Access by Applying the Following Concepts/Methodology/Techniques
- B. Understand and Identify Access Control Attacks (Brute Force, Dictionary, Spoofing, Denial of Service, etc.)
- C. Design, Coordinate and Evaluate Penetration Test

II. Telecommunications & Network Security
- A. Establish Secure Voice and Facsimile Communications
- B. Establish Secure Data Communications
- C. Understand Secure Internet, Intranets, and Extranets
- D. Telecommunications Security Management & Techniques
- E. Prevent Attacks and Control Potential Attack Threats (e.g.; Malicious Code, Flooding, Spamming)
- F. Remote access protocols (e.g., PPP/CHAP/PAP/EAP)
- G. Practice Questions

III. Security Management Practices
- A. Understand goals, mission, and objectives of the organization(s)
- B. Understand the Concepts of Availability, Integrity and Confidentiality
- C. Develop a Security Plan/Policy
- D. Define Roles, Responsibilities and Organization (e.g., separation of duties)
- E. Implement Service Level Agreements
- F. Develop and Implement Standards, Guidelines, and Procedures
- G. Risk Management Concepts
- H. Evaluate Personnel Security
- I. Understand Change Control/ Configuration Management Concepts (e.g., Hardware/ Software)
- J. Conduct Security Awareness and Training
- K. Understand Data Classification Concepts
- L. Evaluate Information System Security Strategies
- M. Certification and Accreditation
- N. Privacy
- O. P. Security Assessment

IV. Applications & systems Development Security
- A. Understand the System Life Cycle and Security (Cradle to Grave)
- B. Databases and Data Warehousing Vulnerabilities, Threats and Protections
- C. Application & System Development Knowledge Security-Based Systems (e.g., expert systems)
- D. Application and System Vulnerabilities and Threats
- E. Practice Questions & Testing

V. Cryptography
- A. Applications and uses (e.g., confidentiality, integrity, non-repudiation)
- B. Methods of Encryption
- C. Define Cryptographic Concepts
- D. Public Key Infrastructure (PKI) (e.g. Certification Authorities, etc.)
- E. Digital Signatures/ Non-repudiation
- F. Message Digests (e.g., MD5, SHA-1)
- G. Cryptanalytic Techniques
- H. Internet Security (e.g., SSL)
- I. Email Security (e.g., PGP, PEM)
- J. Alternatives (e.g., steganography and watermarking)

VI. Security Architecture Models
- A. Understand the Theoretical Concepts of Security Models
- B. Understand the Components of Information Systems Evaluation Models
- C. Understand the Elements of Technical Platforms
- D. Understand how the Security Architecture is affected by certain attacks
- E. Practice Questions

VII. Operations Security
- A. Apply Concepts to Daily Activities
- B. Employ Resource Protection
- C. Handle Violations, Incidents, and Breaches and Report When Necessary
- D. Ensure Administrative Management and Control
- E. Respond to Attacks

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

Certified Information Systems Security Professional-CISSP

Course Outline (cont'd)

VIII. Business Continuity & Disaster Planning

A. Business organization analysis
B. Resource requirements
C. Business impact analysis
D. Recovery strategy
E. Plan design and development
F. Implementation
G. Restoration
H. Review - Assorted Practice Questions & Testing

IX. Law, Investigations, and Forensics & Ethics

A. Identify International Laws that Pertain to Information Systems Security
B. Understand the Parameters of Investigations
C. Understand Forensic Procedures
D. Understand Professional Ethics
E. Understand Major Legal Systems (e.g., Common Law, Civil Law, Islamic, Socialist)
F. Physical Security
G. Restricted areas/ work areas security
H. Escort requirements/ visitor control
I. Turnstiles and mantraps
J. Security guards
K. Badges, Smart/ Dumb Cards, Keys and locks
L. Site selection and facility design configuration
M. Intrusion detection system (e.g., motion detectors, sensors, alarms, CCTV)
N. Audit trails/access logs & intrusion detection
O. Biometric access controls to facility
P. Power and HVAC considerations
Q. Water issues-leakage, flooding
R. Fire detection and suppression
S. Natural disasters
T. Data center security
U. Enterprise identity management
V. Threats
W. Perimeter and building grounds protections
X. Portable Devices and Components
Y. Final review & Questions

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