CISSP Exam Preparation Boot Camp (with exam)

Course Summary

Description

This intensive boot camp provides, detailed instruction, with thousands of exam preparation questions, and includes the exam voucher.

The Certified Information Systems Security Professional (CISSP®) certification provides information security professionals with not only an objective measure of competence but also a globally recognized standard of achievement. This designation is the first credential accredited by ANSI to ISO Standard 17024:2003 in the field of information security.

The CISSP credential demonstrates competence in the 10 domains of the International Information Systems Security Certification Consortium (ISC)² CISSP® CBK®.

Topics

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security

Audience

This course is designed for professionals seeking comprehensive knowledge of security and possibly CISSP certification

Prerequisites

There are no pre-requisites to attend the seminar. However, not everyone will be qualified to take the exam or receive certification.

Certified Professional Exams

This course will help the student prepare for the following exam:

- CISSP Certified Information Systems Security Professional

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

CISSP Exam Preparation Boot Camp (with exam)

Course Outline

I. Access Control
- A. Introduction to Access Control
- B. Definitions and Key Concepts
- C. Information Classification and Access Control
- D. Information Protection Requirements
- E. Information Protection Environment
- F. Security Technology and Tools
  1. Centralized Access Control Methodologies
  2. Decentralized/Distributed Access Control Methodologies
  3. Access to Data
- G. Access Control Categories and Types
- H. Access Control Threats
- I. Access Control Technologies
- J. Assurance Mechanisms
- K. Assurance, Trust, and Confidence Mechanisms
- L. Intrusion Detection
- M. Information Protection and Management Services
- N. CBK
  1. Components
  2. Examples

II. Application Security
- A. Introduction to Application Security
- B. Information Protection Requirements
  1. The C-I-A Triad
- C. Information Protection Environment
  1. Open Source Code and Closed Source Code
  2. Software Environment
  3. The Database and Data Warehousing Environment
  4. DBMS Architecture
  5. Databases and Data Warehouses
  6. Database Interface Languages
  7. Security Assertion Markup Language (SAML)
  8. Data Warehousing
  9. Database Vulnerabilities and Threats
- D. Security Technology and Tools
  1. System Life Cycle and Systems Development
  2. System (Software) Development Methods
  3. Including Security in a Systems Development Method
  4. Programming Language and Security
  5. Software Protection Mechanisms
  6. DBMS Controls
- E. Assurance, Trust, and Confidence Mechanisms
  1. Information Integrity
  2. Information Accuracy
  3. Information Auditing
  4. Evaluation/Certification and Accreditation
- F. Applications Systems Threats and Vulnerabilities
- G. Applications Security Controls
- H. Information Protection and Management Services
  1. Configuration Management
  2. Summary
- I. CBK
  1. Components
  2. Examples

III. Business Continuity and Disaster Recovery Planning
- A. Introduction to Business Continuity and Disaster Recovery Planning
- B. Defining a Disaster
- C. Information Protection Requirements
- D. Information Protection Environment
- E. Project Scope Development and Planning
- F. Business Impact Analysis
- G. Emergency Assessment
- H. Continuity and Recovery Strategy
- I. Plan Design and Development
- J. Implementation
- K. Restoration
- L. Plan Management
- M. Security Technology and Tools
  1. Phase I: Project Management and Initiation
  2. Phase II: Business Impact Analysis (BIA)
  3. Phase III: Recovery Strategies

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 Exam Preparation Boot Camp (with exam)

Course Outline (cont'd)

4. Phase IV: Plan Development and Implementation
5. Phase V: Testing, Maintenance, Awareness, and Training

N. Assurance, Trust, and Confidence Mechanisms
O. Information Protection and Management Services
6. Summary
P. CBK
1. Components
2. Examples

IV. Cryptography
A. Introduction to Cryptography
B. Key Concepts and Definitions
C. History
D. Information Protection Requirements
1. The C-I-A Triad
E. Information Protection Environment
1. Introduction
2. Definitions
3. Cryptanalysis and Attacks
4. Import/Export Issues
F. Security Technology and Tools
1. Basic Concepts of Cryptography
2. Encryption Systems
3. Symmetric Key Cryptography Algorithms
4. Asymmetric Key Cryptography Algorithms
5. Message Integrity Controls
G. Assurance, Trust, and Confidence Mechanisms
1. Digital Signatures and Certificate Authorities
2. Public Key Infrastructure (PKI)
H. Management of Cryptographic Systems
I. Information Protection and Management Services
1. Key Management
2. Key Management Functions
3. Key Generation
4. Distribution
5. Installation
6. Storage
7. Change
8. Control
9. Disposal
10. Modern Key Management
11. Principles of Key Management
12. Summary
J. Threats and Attacks
K. CBK
1. Components
2. Examples

V. Information Security and Risk Management:
A. Introduction to Information Security Management
B. Purposes of Information Security Management
C. Concepts: Confidentiality, Integrity, Availability
D. Risk Analysis and Assessment
1. Information Protection Requirements
2. Information Protection Environment
3. Security Technology and Tools
4. Assurance, Trust, and Confidence Mechanisms
5. Information Protection Management Service
E. Information Classification
1. Information Protection Requirements
2. Information Protection Environment
3. Security Technology and Tools
4. Assurance, Trust, and Confidence Mechanisms
5. Information Protection and Management Services
F. Policies, Procedures, Standards, Baselines, Guidelines
1. Information Protection Requirements
2. Information Protection Environment
3. Security Technology and Tools
4. Information Protection Requirements
G. Security Awareness Training and Education
1. Information Protection Environment
H. Social Engineering
I. Risk Management

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 Exam Preparation Boot Camp (with exam)

Course Outline (cont'd)

J. Ethics
K. Implementation (Delivery) Options
   1. Security Technology and Tools
   2. Assurance, Trust, and Confidence Mechanisms
   3. Information Protection Management Services
L. CBK
   1. Components
   2. Examples

VI. Legal, Regulations, Compliance and Investigations

A. Introduction to Law
B. Major Legal Systems
C. Legal Concepts
   1. Information Protection Requirements
   2. Information Protection Environment
   3. Privacy
   4. Recommended Course of Action
   5. Security Technology and Tools
   6. Assurance, Trust, and Confidence Mechanisms
   7. Information Protection and Management Services
D. Introduction to Regulations
   1. Regulatory Issues
E. Introduction to Investigations
F. Information Protection Requirements
   1. Information Protection Environment
   2. Security Technology and Tools
   3. Assurance, Trust, and Confidence Mechanisms
   4. Information Protection and Management Services
   5. Introduction to Computer Forensics
   6. Introduction to Ethics
   7. Information Protection Requirements
   8. Computer Ethics
   9. Information Protection Environment
   10. Security Technology and Tools
   11. Assurance, Trust and Confidence Mechanisms
   12. Information Protection and Management Services
   13. Summary
G. CBK
   1. Components
   2. Examples

VII. Operations Security

A. Introduction to Operations Security
B. Information Protection Requirements
   1. Resource Protection
C. Information Protection Environment
D. Security Technology and Tools
   1. Change Control Management
   2. Physical Security Controls
   3. Privileged Entity Control
E. Assurance, Trust, and Confidence Mechanisms
F. Information Protection and Management Services
   1. Summary
G. CBK
   1. Components
   2. Examples

VIII. Physical (Environmental) Security

A. Introduction to Physical (Environmental) Security
B. Definitions and Key Concepts
C. Layered Defense Model
D. Information Protection Requirements
   1. The C-I-A Triad
E. Information Protection Environment
   1. Site Location
   2. Equipment Protection
   3. Crime Prevention through Environmental Design (CPTED)
F. Infrastructure Support Systems
G. Security Technology and Tools
   1. Perimeter and Building Grounds Boundary Protection
   2. Building Entry Points
   3. Inside the Building: Building Floors, Office Suites, and Offices
   4. Penetration (Intrusion) Detection Systems
H. Assurance, Trust, and Confidence Mechanisms
   1. Drills/Exercises/Testing

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 Exam Preparation Boot Camp (with exam)

Course Outline (cont'd)

2. Vulnerability/ Penetration Tests
3. Creating a Checklist
4. Maintenance and Service

I. Information Protection and Management Services
1. Awareness and Training
2. Summary

J. CBK
1. Components
2. Examples

IX. Security Architecture and Design

A. Introduction to Security Architecture and Design
B. Components and Principles
1. Hardware
2. Software
C. System Security Techniques
D. Information Protection Requirements
E. The C-I-A Triad
F. Information Protection Environment
1. Platform Architecture
2. Network Environment
3. Enterprise Architecture
4. Security Models
G. Security Technology and Tools
1. Network Protection
H. Assurance, Trust, and Confidence Mechanisms
1. Trusted Computer Security Evaluation Criteria (TCSEC)
2. The Trusted Network Interpretation (TNI)
3. Information Technology Security Evaluation Criteria (ITSEC)
4. The Common Criteria (CC)
5. Certification and Accreditation
I. Security Models and Architecture Theory
J. Security Evaluation Methods and Criteria
K. Information Protection and Management Services
L. CBK
1. Components
2. Examples

X. Telecommunications and Network Security

A. Introduction to Telecommunications and Network Security
B. Key Concepts and Definitions
C. Information Protection Requirements
D. Information Protection Environment
1. Data Networks
2. Remote Access Services
3. Network Protocols
4. Network Threats and Attacks
5. Network Components
6. Telephony
E. Security Technology and Tools
1. Content Filtering and Inspection
2. Intrusion Detection
F. Assurance, Trust, and Confidence Mechanisms
G. Information Protection and Management Services
H. CBK
1. Components
2. Examples
I. Conclusion

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