

The (ISC)²[®] CISSP[®] CBK[®] Review Seminar - 5 Days

Course 958 Overview

- You Will Learn How To**
- Prepare for CISSP Certification based on the (ISC)2 CBK
 - Identify the access control mechanisms that create a security architecture and protect assets
 - Examine core elements of network security including network structures and transmission methods
 - Inspect the key security concepts for software development
 - Recognize the cryptography principles, means and methods of disguising information
 - Explore business continuity and disaster recovery planning for the preservation of business operations
- Course Benefits** This course provides a comprehensive overview of information security concepts and industry best practices and is the only review course endorsed by (ISC) ;. In this course, you cover the ten CISSP domains as outlined in the (ISC) ; CBK and analyze the latest information-system security issues. You also develop an individual study plan to enhance your exam preparation skills.
- Who Should Attend** Security professionals, government and military personnel seeking IAT-3, IAM-2 or IAM-3, IASAE Level 1 or IASAE Level 2 certification to fulfill the DoD 8570.1 Directive, network security personnel and managers. Participants should be aware of the exam eligibility criteria established by (ISC) ;.
- Workshop Course** Throughout this course, you get an in-depth review of the ten CISSP domains as outlined by the (ISC) ; CBK. Workshops include:
- Reviewing the ten domains of the CBK including software development and network security and cryptography
 - Uncovering areas to further develop and expand your exam preparedness
 - Investigating the latest information-system security issues, concerns and countermeasures
 - Reinforcing key areas of the CBK through numerous review sessions

The (ISC)²® CISSP® CBK® Review Seminar - 5 Days

Course 958 Outline

Introduction to (ISC) ; and the exam process

- The CIA (confidentiality, integrity, availability) triad
- Security awareness training and education
- Ethics: personal, corporate, professional

Access Control

Applying concepts, methodologies and techniques to control access

- Types of controls: preventive, detective, corrective
- Decentralized/distributed access control techniques

Access control attacks

- Threat modeling, asset valuation and vulnerability analysis
- Identity and access provisioning life cycle

Telecommunications and Network Security

Secure network architecture and design

- IP and non-IP protocols
- Implications on multi-layer protocols

Securing network components

- Modems
- Switches
- Routers
- Wireless access points
- Network access control devices

Establish secure communication channels

- Voice: POTS, PBX, VoIP
- Remote access: screen scraper, virtual desktop, telecommuting
- Network attacks: DDoS and spoofing

Information Security Governance and Risk Management

Align security function to organizational goals, mission and objectives

- Apply concepts of confidentiality, integrity and availability
- Manage the information life cycle and third-party governance

Risk management concepts

- Identify threats and vulnerabilities
- Countermeasure selection and personnel security management

Software Development Security Security in the software development life cycle

- Operation and maintenance
- Application environment and security controls

Assess the effectiveness of software security

- Security issues of source code and programming languages
- Configuration management

Cryptography

Cryptographic life cycle and encryption concepts

- Foundational
- Symmetric
- Asymmetric
- Hybrid
- Message digests
- Hashing

Integrity controls

- Methods of cryptanalytic attacks
- Cryptographic systems: keys, recovery, PKI and trust models

Security Architecture and Design Components and principles

- Confidentiality
- Integrity
- Multi-level models
- Information systems security evaluation models

Vulnerabilities of security architectures

- Covert channels
- State attacks
- Emanations
- Countermeasure principles, defense in depth

Operations Security

Security operation concepts

- Least privilege
- Special privileges
- Job rotation
- Media and asset management

Preventative measures against attacks

- Malicious code
- Zero-day exploit
- Denial of Service

- System resilience and fault tolerance requirements

Business Continuity and Disaster Recovery Planning

Project scope development and planning

- Business impact analysis
- Continuity and recovery strategy
- Disaster recovery access

Legal, Regulations, Investigation and Compliance

Major legal systems

- Intellectual property
- Computer crime

Ethics: personal, corporate, professional

- (ISC) ; Code of Professional Ethics
- Compliance requirements and procedures

Physical (Environmental) Security

- Site and facility design considerations
- Physical access control and monitoring
- Implementation and operation of facilities and equipment security