



Course Outline: CISSP Security Professional

Total Items: 5 Total Time: 24.00 hour(s)

Summary:

This series helps a learner prepare to take and pass the Certified Information Systems Security Professional (CISSP) exam. This series, like the exam, covers ten domains of information system security knowledge including access control systems and methodology, network and telecommunications security, security management and practices, applications and systems development security, cryptography, security and architecture models, operations security, business continuity and disaster recovery planning, law, investigation, and ethics, as well as physical security.

Certification:

The test that this series prepares students to take is a part of earning the Certified Information Systems Security Professional (CISSP) certification.

Audience:

This series is for anyone preparing for the CISSP exam, or for anyone who wants to learn more about information security subjects.

Features:

- A glossary provides a reference for definitions of unfamiliar terms.
- A skill assessment generates a customized learning path based on the results of a pre-test.

Includes

- Access Control Systems and Methodology 2.0 hour(s)
- Telecommunications and Network Security 3.0 hour(s)
- Security Management and Practices 2.0 hour(s)
- Applications and Systems Development Security 3.0 hour(s)
- Cryptography, Security Architecture, and Security Models 2.0 hour(s)
- Operations Security 2.0 hour(s)
- Business Continuity and Disaster Recovery Planning 2.0 hour(s)
- Law, Investigation, Ethics, and Physical Security 3.0 hour(s)
- Practice Exams 5.0 hour(s)

Detailed Course Items

Includes:

Access Control Systems and Methodology

Objectives:

- Discuss the relationship between access control and accountability
- Define common access control techniques and models
- Detail the specifics of access control administration
- Explain identification and authentication techniques
- Discuss centralized/decentralized control
- Explain intrusion detection and common methods of attack

Topics:

- Authentication, access control, and accountability
- Access control techniques
- Access control administration and models
- Identification and authentication techniques
- Access control methodologies
- Methods of attacks
- Monitoring
- Penetration testing

Telecommunications and Network Security**Objectives:**

- Explain the International Standards Organization/Open Systems Interconnection (ISO/OSI) layers and characteristics
- Describe the design and function of communications and network security
- Describe the components, protocols and services involved in Internet/intranet/extranet design
- Define and describe communications security techniques to prevent, detect, and correct errors so that integrity, availability, and confidentiality of transactions over networks may be maintained
- Define and describe specific areas of communication and how they can be secured
- Explain current forms of network attacks and their countermeasures

Topics:

- The Open Systems Interconnection model
- Network characteristics
- Network topologies
- LAN devices
- WAN technologies
- Providing remote access capabilities
- Networking and security protocols
- Securing communications
- Error prevention, detection, and correction
- Intrusion detection, response, and prevention
- Fault tolerance and data restoration

Security Management and Practices**Objectives:**

- Understand the principles of security management
- Understand risk management and how to use risk analysis to make information security management decisions
- Set information security roles and responsibilities throughout your organization
- Understand the considerations and criteria for classifying data
- Determine how employment policies and practices are used to enhance information security in your organization
- Use change control to maintain security

Topics:

- Defining security principles
- Identification and authentication
- Accountability and auditing
- Security management planning

- Risk management and analysis
- Risk analysis step by step
- Policies, standards, guidelines, and procedures
- Examining roles and responsibility
- Understanding protection mechanisms
- Classifying data
- Employment policies and practices
- Managing change control
- Security awareness training

Applications and Systems Development Security

Objectives:

- Demonstrate an understanding of challenges in both distributed and nondistributed environments
- Discuss databases and data warehousing issues
- Describe knowledge-based systems and examples of edge computing
- Discuss the types of attacks made on software vulnerabilities
- Describe and define malicious code
- Discuss system development controls

Topics:

- Distributed and nondistributed environment challenges
- Database and data warehousing issues
- Storage and storage systems
- Knowledge-based systems and edge computing
- Attacking software
- Understanding malicious code
- System development lifecycle models
- Security control architecture
- Software development methodologies
- Secure software design and coding practices

Cryptography, Security Architecture, and Security Models

Objectives:

- Compare and contrast symmetric and asymmetric algorithms
- Describe PKI and key management
- Detail common methods of attacking encryption, including general and specific attacks
- List common security models and their function
- Explain the basics of security architecture
- Describe the Internet Protocol Security (IPSec) standard

Topics:

- Uses of cryptography
- Cryptographic concepts, methodologies, and practices
- Methods of attack
- Security architecture and model requirements
- Security models
- Security system architecture
- Information system security standards
- Common criteria
- IPSec

Operations Security

Objectives:

- Identify the key roles of operations security
- Define threats and countermeasures
- Explain how audit and monitoring can be used as operations security tools
- Define the role of Administrative management in operations security
- Define operations security concepts and describe operations security best practices

Topics:

- Key operations security roles
- The roles of auditing and monitoring
- Penetration testing techniques
- Defining threats and countermeasures
- Countermeasures for employee-related threats
- The role of administrative management
- Concepts and best practices

Business Continuity and Disaster Recovery Planning

Objectives:

- Document the natural and man-made events that need to be considered in making disaster recovery and business continuity plans
- Explain the difference between disaster recovery planning (DRP) and business continuity planning (BCP) and the importance of developing plans that include both
- Detail the business continuity planning process
- Explain the need for, and development of, a backup strategy. Include information on determining what to back up, how often to back up, as well as the proper storage facility for backups
- Detail the disaster recovery planning process, including recovery plan development, implementation, maintenance, and the restoration of business functions

Topics:

- Business operation disasters
- DRP and BCP differences
- BCP scope and business impact analysis
- Developing operational plans for BCP
- BCP implementation, testing and maintenance
- Disaster recovery planning
- Developing a backup strategy
- Alternative site requirements

Law, Investigation, Ethics, and Physical Security

Objectives:

- Define what constitutes a computer crime and how such a crime is proven in court
- Explain the laws of evidence
- Discuss computer ethics
- Understand general principles that apply to the theft of information and assets
- Know the general criteria that apply to the location and construction of facilities
- Describe physical intrusion detection methodologies and products

Topics:

- Fundamentals of law
- Criminal law and computer crime
- Computer security incidents
- Legal evidence
- Computer forensics
- Computer ethics
- Classifying assets and vulnerabilities
- Site location and construction
- Physical access controls
- Power
- Environmental controls and water exposure problems
- Fire prevention and protection
- Tape, media, and document library retention policies
- Waste disposal
- Physical intrusion detection

Practice Exams**Objectives:**

- Practice for the Certified Information Systems Security Professional (CISSP) exam

Topics:

- Certification process overview
- Exam prep tips
- Fast facts
- Practice Exam 1
- Practice Exam 2
- Practice Exam 3
- Practice Exam 4
- Practice Exam 5