# Certified Information Systems Security Profession E-Learning

**Duration: 1 Day** **Course Code: E-CISSP**

## Overview:

Certified Information Systems Security Professional (CISSP) certification has been developed and maintained by (ISC)2, a not-for-profit leader in educating and certifying information security professionals. CISSP was the first information security credential and is aimed at professionals who develop policies and procedures in information security. CISSP is accredited by the American National Standards Institute (ANSI) to International Organization for Standardization (ISO) Standard 17024:2003.
This course includes new content that will provide a thorough understanding of the topics covered on the CISSP exam.

## Target Audience:

IT consultants, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, security engineers, and other security professionals whose positions require CISSP certification.

## Objectives:

- Access control
- Telecommunications and network security
- Information security governance and risk management
- Software development security
- Cryptography
- Security architecture and design
- Security operations
- Business continuity and disaster recovery planning
- Legal, regulations, investigations, and compliance
- Physical (environment) security

## Prerequisites:

- Systems administration experience, familiarization with TCP/IP, and an understanding of UNIX, Linux, and Windows. This advanced course also requires intermediate-level knowledge of the security concepts covered in our Security+ Prep Course.
- Security+ Prep Course (SYO-301)

## Testing and Certification

- This course is part of the following programs or tracks:
- CISSP - Certified Information Systems Security Professional

## Follow-on-Courses:

- CISA Prep Course
- CISM Prep Course

## Content:

### 1. Access Control

- Critical activities related to information classification
- Knowledge-based authentication technologies
- Characteristic-based authentication technologies
- Single Sign-On Systems (SSOs)
- One-Time Passwords (OTPs) and smart cards
- Securing passwords
- Attacks against passwords and password files
- Evaluate given passwords
- Appropriate access control models
- Features of the discretionary access control (DAC) and mandatory access control (MAC) models
- Techniques that control access to resources
- Advantages and disadvantages of centralized and decentralized identity management systems
- Intrusion detection system (IDS) mechanisms and implementation methods
- Intrusion detection and prevention techniques
- Access control and intrusion detection techniques

### 2. Telecommunications and Network Security

- Components of a network infrastructure
- Key features of firewall technologies
- Characteristics of TCP/IP
- Layers of the OSI model and their functions
- How specific network attack techniques operate
- High-level security solution
- Network interaction
- Types of cable
- LAN transmission considerations
- Network topology characteristics
- Features of media access technologies
- Synchronous and asynchronous communications
- LAN and WAN specific devices and technologies
- Packet-switched networks
- Remote access protocols and their functions
- Characteristics of Ethernet
- Data transmission in Token Ring networks
- Characteristics of the network communications mechanisms
- Technologies used in an enterprise environment
- VPN protocols
- Network communication solutions
- Network protocols
- Transport layer mechanisms to secure network data

### 4. Software Development Security

- Issues related to software development and how they create security vulnerabilities
- Types of attacks used in the enterprise environment
- Appropriate methods to counteract an attack
- Types of computer attacks
- Types of malicious code
- Purpose of software forensics
- Antivirus software
- Steps to counteract a given attack
- Characteristics of knowledge-based systems
- Development models
- Database models and technologies
- Software development phases

### 5. Cryptography

- Cryptographic terms
- Characteristics of quantum cryptography
- Symmetric algorithms
- Asymmetric algorithms
- Message formats
- Ciphers
- Cryptanalytic attacks
- Algorithms, message formats, ciphers, and cryptanalytic attacks
- Cryptography implementation
- Hash algorithms
- Message authentication codes
- Digital signatures
- Guidelines for key management and distribution
- XKMS
- Split knowledge method of key management
- Key distribution
- Actions of an individual who is practicing key management
- Key management methods

### 6. Security Architecture and Design

- Basic information system architecture
- Implementing security architecture
- CPU operational factors involved in secure addressing
- System operating states
- Machine types
- Resource manager
- RAM vs. ROM
- Storage types
- Securing computer networks
- Network resources required
- Phases of the evaluation process
- Essential features of operating system protection
- Access control mechanisms
- Methods to evaluate security in a networking environment

### 8. Business Continuity and Disaster Recovery Planning

- Project initiation phase of business continuity planning
- Business continuity and disaster recovery planning
- Business impact analysis
- Considerations when conducting a business impact analysis
- Initiating a project to plan a business continuity and disaster recovery program
- Steps of a business impact analysis
- Considerations weighed when determining an appropriate recovery strategy
- Recovery strategies for business operations
- Recovery strategies for technology environments
- Components of a business continuity and disaster recovery plan
- Test type purposes
- Recovery strategies
- Elements of a business continuity and disaster recovery plan

### 9. Legal, Regulations, Investigations, and Compliance

- Major categories of computer crime
- Characteristics of various computer-related crimes
- Intellectual property laws
- Laws related to information security and privacy
- Types of computer crimes
- Due care and due diligence
- Computer crime investigations
- Investigative considerations involved in dealing with computer crime
- Ethics vs. ethical fallacies
- Processes for investigating a computer-related crime

### 10. Physical (Environment) Security

- Threats to an organization's physical security
- Components of a layered defense system
- Perimeter security mechanisms
- Physical security considerations when designing or building a facility
- CPTED strategies
- Security solutions
- Design measures taken to increase facility security
- Mechanisms and controls for securing building services
- Technologies used by an IDS
- Intrusion detection technology
- Characteristics of a compartmentalized area
- Strategies for securing compartmentalized areas

- Different technologies used to protect data at the application layer
- Secure network communications
- Secure transport technologies vs. application layers

**3. Information Security Governance and Risk Management**

- Information security risk management
- Principles and how to apply them
- Components of a policy framework
- Methodological frameworks for implementing and auditing security controls
- Methodological frameworks for performing information security risk assessment
- Results of qualitative and quantitative risk assessments
- Stages of the risk assessment process
- Avoidance, transfer, mitigation, or acceptance
- Application of risk management concepts
- Risk assessment and control methodologies
- Responsibilities of an Information Security Officer
- Advantages and disadvantages of various reporting models
- Personnel security strategies to minimize employee risk
- Strategies for implementing information security training
- Topics a computer ethics program should address
- Common computer ethics fallacies
- Ethical principles that all information security professionals should apply
- Handling organizational issues
- Appropriate actions to implement security awareness training in your organization
- Ethical principles that all information security professionals must apply
- Features of security models
- Peer-to-peer security issues
- Security issues associated with grid computing
- Challenges to securing data in the cloud
- Questions a user of cloud data storage needs to ask when conducting a risk assessment
- Operating system security solutions
- Security in a networking environment
- Security challenges from distributed systems

**7. Security Operations**

- Securing the operations of an enterprise
- Internal or external audit measures
- Technologies used to maintain resource availability
- Attack type effects
- Approaches to securing operations
- Audit trails used in operations security
- Monitoring tools vs. techniques
- Strategies for securing and maintaining resources
- Securing enterprise operations against network violations
- Operations security
- Resource protection
- E-mail protocols
- E-mail vulnerability
- Security issues associated with the web interfacing
- Transferring and sharing files over the Internet
- Reconnaissance methods
- Considerations involved in implementing administrative controls
- Securing media and media storage devices
- Reasons resource and e-mail should be secure
- Safer file sharing practices
- How to secure media
- Features of physical security elements
- Fundamental considerations involved in key control
- Best approach to securing building services
- Secure a facility and its contents
- Implement an effective physical barrier as a security measure

## Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.co.uk

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK