Certified Information Systems Security Professional (CISSP)

Modality: Virtual Classroom

Duration: 5 Days

About this Course:

The CISSP Certification is one of the most well-worth certifications in the niche of information security. The certification serves as a testimony of the professionals' managerial and technical knowledge and capabilities and validates his extensive working experience relating to managing, designing, and engineering the organizations' security infrastructure. On average, a CISSP Certified Security Specialist earns $126,770 annually. This course provides professionals with the fundamental knowledge of the CISSP exam and helps develop a better understanding of the 8 domains of CISSP.

Course Objectives:

The CISSP Exam is based on the 8 information security domains that play a substantial role in augmenting the standards of security in national infrastructure, corporations, and information systems. The primary objective of these distinguished domains is to help professionals develop a sound knowledge and understanding of the information security needs of a business enterprise. With the integration of human, managerial, and technical aspects, the CISSP exam strives to build better collaboration between system and information security. The eight domains of the CISSP Common Body of Knowledge (CBK) include Security and Risk Management, Security Engineering, Asset Security, Identity and Access Management, Communication and Network Security, Security Assessment and Testing, Software Development Security, and Security Operations.

Audience:

The following group of professionals can relish the maximum benefits from the learnings and certification of CISSP:

- Security Manager
- Network and Security Architect
- IT Manager and Security Director
- Security System Engineer
- Information Security Professionals
- Security Analyst and Consultant

Prerequisites:

- Candidates must have 4-year Graduate Degree or Equivalent
- A minimum of 5 years of working experience in multiple CISSP-CBK domains is mandatory
- The $(ISC)^2$ Approved List Credential Credit will account for 1-year experience
- Inexperienced Candidates can become $(ISC)^2$ Associate by passing CISSP Exam
- The $(ISC)^2$ Associate must earn 5 years working experience in the next 6 years.

Suggested Prerequisites:

- CompTIA Security+ (Exam SY0-401)
- Information System Certification and Accreditation Expert
- Certified Information Systems Security Professional – Overview

Course Outline:

1. Security Management Practices

- Types of Security Controls
- Components of a Security Program
- Security Policies, Standards, Procedures, and Guidelines
- Risk Management and Analysis
- Information Classification
- Employee Management Issues
- Threats, Vulnerabilities and Corresponding Administrative Controls

2. Access Control Systems and Methodology

- Identification, Authentication, and Authorization Techniques and Technologies
- Biometrics, Smart Cards, and Memory Cards
- Single Sign-On Technologies and Their Risks
- Discretionary versus Mandatory Access Control Models
- Rule-based and Role-based Access Control
- Object Reuse Issues and Social Engineering
- Emissions Security Risks and Solutions
- Specific Attacks and Countermeasures

3. Cryptography

- Historical Uses of Cryptography
- Block and Stream Ciphers
- Explanation and Uses of Symmetric Key Algorithms
- Explanation and Uses of Asymmetric Key Algorithms
- Public Key Infrastructure Components
- Data Integrity Algorithms and Technologies
- IPSec, SSL, SSH, and PGP
- Secure Electronic Transactions
- Key Management
- Attacks on Cryptosystems

4. Physical Security

- Facility Location and Construction Issues
- Physical Vulnerabilities and Threats
- Doors, Windows, and Secure Room Concerns

- Hardware Metrics and Backup Options
- Electrical Power Issues and Solutions
- Fire Detection and Suppression
- Fencing, Lighting, and Perimeter Protection
- Physical Intrusion Detection Systems

5. Enterprise Security Architecture

- Critical Components of Every Computer
- Processes and Threads
- The OSI Model
- Operating System Protection Mechanisms
- Ring Architecture and Trusted Components
- Virtual Machines, Layering, and Virtual Memory
- Access Control Models
- Orange Book, ITSEC, and Common Criteria
- Certification and Accreditation
- Covert Channels and Types of Attacks
- Buffer Overflows and Data Validation Attacks

6. Law, Investigation, and Ethics

- Different Ethics Sets
- Computer Criminal Profiles
- Types of Crimes
- Liability and Due Care Topics
- Privacy Laws and Concerns
- Complications of Computer Crime Investigation
- Types of Evidence and How to Collect It
- Forensics
- Legal Systems

7. Telecommunications, Networks, and Internet Security

- TCP\IP Suite
- LAN, MAN, and WAN Topologies and Technologies
- Cable Types and Issues
- Broadband versus Baseband Technologies
- Ethernet and Token Ring
- Network Devices
- Firewall Types and Architectures
- Dial-up and VPN Protocols
- DNS and NAT Network Services
- FDDI and SONET
- X.25, Frame Relay, and ATM
- Wireless LANs and Security Issues
- Cell Phone Fraud
- VoIP

- Types of Attacks

8. Business Continuity Planning

- Roles and Responsibilities
- Liability and Due Care Issues
- Business Impact Analysis
- Identification of Different Types of Threats
- Development Process of BCP
- Backup Options and Technologies
- Types of Offsite Facilities
- Implementation and Testing of BCP

9. Applications & Systems Development

- Software Development Models
- Prototyping and CASE Tools
- Object-Oriented Programming
- Middleware Technologies
- ActiveX, Java, OLE, and ODBC
- Database Models
- Relational Database Components
- CGI, Cookies, and Artificial Intelligence
- Different Types of Malware

10. Operations Security

- Operations Department Responsibilities
- Personnel and Roles
- Media Library and Resource Protection
- Types of Intrusion Detection Systems
- Vulnerability and Penetration Testing
- Facsimile Security
- RAID, Redundant Servers, and Clustering?