Certified Information Systems Security Professional (CISSP)

Modality: Virtual Classroom

Duration: 5 Days

About this course:

One of the globally recognized certifications in the information security industry is “The Certified Information Systems Security Professional (CISSP).” Through the certification, an individual will be able to get extensive technical and managerial knowledge along with experience in regard to effectively maintaining the overall security environment of an organization through efficient designing, engineering, and management skills.

The course will help in gaining fundamental knowledge, which is required to sit for (ISC)2® Certified Information Systems Security Professional (CISSP®) exam. The course is designed in line with CISSP CBK 8 domains and provides a comprehensive understanding of the broad spectrum of the domains. Through the certification, a professional can efficiently and adequately protect information systems, corporations, and national infrastructure.

Information security is a vital part of every organization these days and failing to provide a secure environment has led to many mishaps. Understanding and implementation of the CISSP CBK domains help in constructing a secure environment through effectively coordinating technical, managerial and human factors.

The expected annual salary for a CISSP Certified IT Security Specialist is **$126,770**/- per annum.

Course Objectives:

The objective of the course is not only restricted to providing understanding of the domains but also to highlight and teach the CISSP CBK 8 domains relevancy across all disciplines of the information security field.

CISSP CBK 8 domains are:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Audience:

Following professionals are advised to take the course;

- Security Consultant
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- IT Director/Manager
- Director of Security
- Network Architect
- Security Systems Engineer
- Chief Information Security Office

Prerequisites:

An individual looking forward to taking the CISSP exam must have a minimum of five years of working experience in a job role, which covers at least two or more of the CISSP CBK eight domains. Having a four-year college degree or regional equivalent or an additional credential from the (ISC)² approved list, is equivalent to one year of working experience required.

An individual without having prior experience can also sit for the exam and get certification. However, the individual will be treated as Associate of (ISC)² and can become a certified CISSP after completing six years of relevant experience.

Suggested prerequisites courses:

- Certified Information Systems Security Professional - Overview
- Information Systems Certification and Accreditation Professional
- CompTIA Security+ (Exam SY0-501) (CompTiaSec-SY0-501)

Note: The course is exclusive of the exam voucher. However, if needed, the exam voucher can be purchased by contacting our Support Team.

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?