QUICKSTART
Over 35 Years Of Technology Training

Document Generated: 09/19/2024

Learning Style: Virtual Classroom

Provider:

Difficulty: Intermediate

Course Duration: 5 Days

Next Course Date: **October 21, 2024**

Certified Information Systems Security Professional (CISSP)

About this course:

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional’s deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

In this course, you gain the foundational knowledge to fully prepare for the (ISC)$^{2®}$ Certified Information Systems Security Professional (CISSP$^{®}$) exam, including a comprehensive understanding of the CISSP CBK 8 domains also covers the broad spectrum of topics and ensure its relevancy across all disciplines in the field of information security.

CISSP CBK 8 domains:

• Security and Risk Management • Asset Security • Security Engineering • Communications and Network Security • Identity and Access Management • Security Assessment and Testing • Security Operations • Software Development Security

The average salary for a CISSP Certified IT Security Specialist is **$126,770** per year.

Course Objectives:

The CISSP exam is rigorous, covering eight security domains essential for the protection of information systems, corporations and national infrastructures. Understanding that security is an enterprise wide problem, these domains provide the candidate with a broad understanding of the technical, managerial and human factors that must coordinate effectively to keep information and systems secure. These domains include:

The Eight Domains of the CISSP CBK (Common Body of Knowledge)

- 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:

The CISSP is ideal for those working in roles such as:

- Security Consultant
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect

- IT Director/Manager
- Director of Security
- Network Architect
- Security Systems Engineer
- Chief Information Security Officer

Prerequisites:

- Candidates must have a minimum of 5 years cumulative paid full-time work experience in 2 or more of the 8 domains of the CISSP CBK. Earning a 4-year college degree or regional equivalent or an additional credential from the (ISC)² approved list will satisfy 1 year of the required experience. Education credit will only satisfy 1 year of experience.
- A candidate that doesn’t have the required experience to become a CISSP may become an Associate of (ISC)² by successfully passing the CISSP examination. The Associate of (ISC)² will then have 6 years to earn the 5 years required experience

Suggested prerequisites courses:

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

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?

Credly Badge:

QUICKSTART
Course Name:
Certified Information Systems Security Professional (CISSP) Training
INFORMATION SECURITY

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges