



This course trains students in all areas of the security Common Body of Knowledge (CBK). They will learn about security policy development, secure software development procedures, network vulnerabilities, attack types and corresponding countermeasures, cryptography concepts and their uses, disaster recovery plans and procedures, risk analysis, crucial laws and regulations, forensics basics, computer crime investigation procedures, physical security, and much, much more. They will explore the contents and concepts that make up the diverse domains and learn how they work together to provide true “in-depth” defense.

CISSP Training package # 1 (6 days) :

1. 5 day classroom based CISSP Certification course
2. Day 6 mentored examination preparation and review
3. 1,500 page student workbook with study materials, practice exams and review content

CISSP Training package # 2 (5 Days):

1. 5 day classroom based CISSP Certification course
2. 1,500 page student workbook with study materials, practice exams and review content

6-Day Course Schedule Overview

This course has been designed to provide all the materials needed for 5 full days of instructor led classroom training, plus 1 day of review, culminating with the administration of the exam on the seventh day or alternative date per individual needs.

Day 1: Security Management Practices; Access Control Systems and Methodology

Day 2: Cryptography; Physical Security

Day 3: Enterprise Security Architecture; Law, Investigation, and Ethics

Day 4: Telecommunications and Network Security; Business Continuity Planning

Day 5: Applications and Systems Development; Operations Security

Optional Day 6: Review of all material in preparation for the CISSP exam.

The coursework is difficult, and the exam is extremely challenging. Students should plan on evening hour study and afterclass work assignments. Study groups are encouraged.

Prerequisites

Anyone may attend this course, but those with experience in one or more of the ten domains will reap the greatest benefits.

WHY PURSUE A CISSP?

Many companies are beginning to regard a CISSP certification as a requirement for their technical, mid-management, and senior IT management positions. Achieving the Certified Information Systems Security Professional (CISSP)—the world's global security certification standard—proves high proficiency in foundation security disciplines. Offered through (ISC)², one of the world's leading international security certification organization, the exam's stringent criteria sets the benchmark for excellence in security practice, requiring candidates to prove deep understanding of security concepts, principles, and methodologies.

The CISSP exam is rigorous, covering ten 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 Ten Domains of the CBK

1. Security Management Practices
2. Access Control Systems and Methodology
3. Cryptography
4. Physical Security
5. Enterprise Security Architecture
6. Business Continuity Planning
7. Telecommunications and Network Security
8. Law, Investigation, and Ethics
9. Applications and Systems Development
10. Operations Security

Using this course, students prepare for the exam, while at the same time obtain essential security knowledge that can be immediately used to improve organizational security. This knowledge enhances services and products, secures business functions and infrastructures, provides better implementation processes, and can be used to restructure critical programs and procedures to help keep companies up-to-date on today's business and security strategies, technologies, and best practices.

Training is an investment, not an expense. A skilled workforce is a competitive asset.

COURSE CONTENTS

What's Included:

A curriculum workbook of 1,500 pages includes:

- 10 modules covering each of the 10 CBK domains
- Professionally developed graphics and 3-D animations that enhance the understanding of complex concepts.
- Extensive notes accompanying each slide, including Configuration Steps, Hints, Warnings, Tips, Tables, etc.
- Quick Tips section, Summary section, Terminology section, and 20 questions and answers for each module.
- Review materials including;
 - o A final practice exam of 400+ questions (in addition to those included in student manual)
 - o A CISSP review booklet
 - o A CISSP cram session

The Ten Domains In Detail:

CISSP candidates are expected to be knowledgeable of the concepts, skills and technologies embodied in each domain. Here is an overview of the range of topics students will explore for each domain:

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. 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

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. 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

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

At Course Completion

Students will emerge from this course, prepared to meet the challenge of CISSP certification exam. Whether or not they choose to take the exam they will have gained a broad understanding of all of the components necessary to provide true security, and will bring this knowledge and these solutions back to the workplace.



For information and registration, call 1-888-296-6682 Ext: 267 or email training@novaknowledge.com