



CISSP® Certification Training

Introduction

Passing the CISSP examination is a challenge. Even the most experienced practitioner runs a high risk of failure if they do not do a significant amount of preparation for this examination. One reason is the sheer breadth and diversity of the content; many of the subtopics of the domains are studies in themselves. The CISSP examination costs \$599.00 per attempt. This training program has been developed to help you to reduce your risk of failure. We have gone to great lengths to ensure that all the material you need to know is covered in a meaningful way that is highly relevant to the practical issues faced by security managers today. In-class diagnostic tests are conducted during and after each section so that you can assess your performance and identify the areas your weak on.

The CISSP has clearly emerged as the key certification for security professionals. In fact, an informal survey of information security jobs on a major employment web site revealed that over 70% of the positions required CISSP certification. Corporations are demanding experienced information security professionals, with the certifications to prove it, to protect their information and assets.

During the training program, through questions and interaction we will help you to judge when you are ready to sit the exam. We will also provide you with a list of on-line resources to help you strengthen and deepen your knowledge in each domain. After the training program you can call on us to answer your questions and provide support until you pass the exam.

Course Objective: To provide students with an in-depth view of Information Security and to provide all the material needed to pass the CISSP certification exam.

Who should attend?

Experienced security professionals who want to expand their knowledge and gain an internationally recognized accreditation. Whilst anyone can attend our seminar, the CISSP accreditation is not available to anyone who does not meet the (ISC)2 entry requirements(see below for requirements).

Prerequisites:

Experienced security professionals who want to expand their knowledge and gain an internationally recognized accreditation. Whilst anyone can attend our seminar, the CISSP accreditation is not available to anyone who does not meet the (ISC)2 entry requirements. We will be happy to advise you on your eligibility.



Delivery Method: Instructor-led, group-paced, classroom-delivery learning model with structured, hands-on activities.

What's in the training program?

The topics reflect the requirements of the ten domains of the Common Body Of Knowledge defined by (ISC)2.

Security Management Practices

- Identification of information assets
- Policies, standards, procedures
- Confidentiality, integrity, and availability.
- Data classification,
- Risk management, risk assessment, and risk analysis;
- Countermeasure evaluation
- Security roles
- Security awareness training
- Personnel policy

Security Architecture & Models:

- Computer architectures
- Security models
- Trusted Computer Base
- ITSEC
- TCSEC
- Common Criteria
- OS security components
- IETF IPSEC
- Certification and Accreditation
- Security issues associated with system architectures

Access Control Systems & Methodology:

- Access Control techniques
- Access Control Administration
- Access Control Models
- Identification and Authentication Techniques
- Single Sign-On (SSO)
- Access Control Methodologies and Implementation
- File and Data Ownership and Custodianship
- Methods of Attack
- Monitoring
- Penetration Testing



Applications & Systems Development:

- Systems development management
- Change Control
- Certification
- Accreditation
- Security Control Architecture
- Malicious Code
- Virus writers Hackers, crackers, and phreaks
- Virus protection, types of computer viruses
- Mobile code security issues

Cryptography:

- Cryptographic basics
- Comparison of cryptographic algorithms
- Key management
- Key Distribution Methods
- Kerberos,
- ISAKMP
- Public Key Algorithms
- Public Key Infrastructure (PKI)
- Certificate Authorities
- Smart cards and tokens
- Methods of Attack

Telecommunications & Network Security:

- ISO/OSI Layers and Characteristics
- Remote Access Dial-In User System/Terminal Access Control
- RADIUS/TACACS
- Internet/Intranet/Extranet
- Secure communication protocols
- Virtual Private Network (VPN)
- Network Address Translation
- E-mail security
- Facsimile security
- Secure Voice Communications
- Security boundaries and how to translate security policy to controls
- Network Attacks and Countermeasures

Operations Security:

- Administrative Management
- Separation of Duties and Responsibilities
- Backup of Critical information
- Standards of Due Care/Due Diligence
- Record retention



- Control Types
- Operations Controls
- Resource Protection
- Auditing
- Reporting mechanisms
- Monitoring tools and techniques
- Failure recognition and response
- Intrusion detection
- Penetration testing techniques
- Inappropriate activities
- Internal threats and Countermeasures
- Violations, Breaches, and Reporting

Physical Security:

- Physical site security controls
- Electronic site access controls
- Environment/Life Safety
- Physical security threats and countermeasures
- Fire (sensors, sprinklers, flooding systems, extinguishers)
- Water (leakage and flooding)
- Electrical (UPS and generators)
- Environmental

Business Continuity & Disaster Recovery Planning:

- Business Continuity Planning
- Cold/Warm/Hot/Mobile Sites
- Recovery processes
- Disaster Recovery Planning
- Recovery Plan Development
- Emergency Response
- Reconstruction from Backups
- Crisis Management
- BCP/DRP Events

Law, Investigation & Ethics:

- Legal categories
- Criminal Law
- Civil Law
- Administrative Law
- Investigations
- Rules of Evidence
- Collection and preservation of evidence
- Investigation Processes and Techniques
- Major categories of computer crime
- Incident Handling



- Ethics
- (ISC2)TM Code of Ethics

Do you have the proper experience for your CISSP credential?

You must have a minimum of five years of direct full-time security work experience in two or more of these 10 domains of the (ISC)² CISSP CBK[®]:

- **Access Control**
Concepts, terms of subjects and objects, implementation of authentication techniques
- **Application Security**
Security and controls of the systems development process, life cycle, application controls, change controls, data warehousing, data mining, knowledge based systems, program interfaces, and concepts used to ensure data and application integrity, security, and availability
- **Business Continuity and Disaster Recovery Planning**
Preservation of the business in the face of major disruptions to normal business operations
- **Cryptography**
Business and security requirements for cryptography, principles of certificates and key management, secure protocols
- **Information Security and Risk Management**
Identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability
- **Legal, Regulations, Compliance and Investigations**
Computer crime laws and regulations, the investigative measures and techniques which can be used to determine if a crime has been committed, methods to gather evidence if it has, as well as the ethical issues and code of conduct for the security professional
- **Operations Security**
Identify the controls over hardware, media, and the operators with access privileges to any of these resources
- **Physical (Environmental) Security**
Threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information
- **Security Architecture and Design**
Concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications,



and those controls used to enforce various levels of confidentiality, integrity, and availability

- **Telecommunications and Network Security**

Structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media

Note that if certain circumstances apply and with appropriate documentation, candidates are eligible to waive one year of professional experience:

- One year waiver of the professional experience requirement based on a candidate's education.
Candidates can substitute a maximum of one year of direct full-time security professional work experience described above if they have a four-year college degree OR Advanced Degree in information security from a U.S. National Center of Academic Excellence in information Security (CAEIAE) or regional equivalent.

OR

- One-year waiver of the professional experience requirement for holding an additional credential on the (ISC)² approved list
Valid experience includes information systems security-related work performed as a practitioner, auditor, consultant, investigator or instructor, that requires Information Security knowledge and involves the direct application of that knowledge.
- The five years of experience must be the equivalent of actual fulltime Information Security work (not just Information Security responsibilities for a five year period); this requirement is cumulative, however, and may have been accrued over a much longer period of time.

Benefits:

Earning an (ISC)² certification puts you in the middle of an elite network of professionals and a vast base of knowledge unparalleled in the information security industry. But the advantages don't stop there. (ISC)² continues to support you throughout your career. Just remember, the only way you can become a member and join the (ISC)² family is by attaining an (ISC)² credential.



Knowledge Center Inc provides a cost-effective, intense training and education solution for individuals and corporation employees alike wanting to enhance and advance their careers. Knowledge Center Inc offers top-quality training that can be custom-tailored to meet an individual student's learning style and specific needs.

With our state-of-the-art facility in Ashburn, VA equipped with latest equipment and an industry-focused approach, training programs encompass in demand multiple industry certifications from a variety of leading technology vendors, along with hands-on practical and interactive education experiences. Specific job skills training, combined with problem solving, critical thinking and other relevant real-world training, provides Knowledge Center Inc trained students the competitive edge and skill sets.

CERTIFIED AND EXPERIENCED INSTRUCTORS!

Our highly qualified instructors hold advanced certifications, including CISSP, CEH, VCP, SCSA, CCNP and MCSE, among others and are highly experienced individuals. They bring with them vast practical experience thereby, offer real-life situations, not just academic "what-if" scenarios.

THE MOST SUPPORTIVE LEARNING ENVIRONMENT

We offer free, pre-training assistance to every student, the best industry certification guarantee, and instruction where you need it: our facility, your facility (Embedded Training Team), or even for your teams in the field (Mobile Training Team).

Knowledge Center Inc delivers innovative in depth content-centered learning solutions and training programs with a unique integrated learning approach, which encompasses more than just "taking a course", Knowledge Center Inc provides a complete method of class room instructor led training, reinforcing after training with after class support and validating by achieving certification.

Pre-Training Preparation

Each student will receive our course materials 7 days prior to start of the CISSP Boot Camp. The students are required to read the material and familiarize themselves with the contents and few important Terms prior to joining the Boot Camp. This will help the students learn better and get maximum benefits from our CISSP Boot Camp. This process of preparation for our training has been found to be very effective in learning the CISSP course materials and passing the CISSP exam.

1 DAY FOR EXAM: We can help you with registration for the exam or you can register for it.



Schedule: Boot Camp, Monday thru Fri 9.00am-5.30pm

Delivery Format: Instructor Led

Price/Candidate: \$2995 all inclusive of the training, study materials, practice exams and one exam voucher.

Payment Terms: Payment must be received in advance at least 10 days before start of training.

Certificate: Certificate of completion will be given to all students who meet the 85% attendance requirement and complete other course work given during training period.