

Course Description:

This course trains students in all areas of the security Common Body of Knowledge. They will learn 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 more.

There are four processes a candidate must successfully complete to become a certified CISSP. To sit for an exam, a candidate must assert that he or she possesses a minimum of five years of professional experience in the information security field or four years of experience plus a college degree. Professional experience has to be in two or more of these 10 (ISC)² CISSP domains: Access Control, Application Development Security, Business Continuity and Disaster Recovery Planning, Cryptography, Information Security Governance and Risk Management, Legal, Regulations, Investigations and Compliance, Operations Security, Physical (Environmental) Security, Security Architecture and Design, and Telecommunications and Network Security.

Who Should Attend:

Students who wish to pass the CISSP certification exam will benefit from this class.

Prerequisites:

There are no prerequisites for this course, although having taken other security courses is extremely helpful.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Confidently meet the challenge of CISSP certification exam

Course Outline:**Access Control Systems and Methodologies**

Access control concepts, methodologies, and implementation
 Access controls: detective, corrective, and preventative
 Access control techniques in centralized and decentralized environments
 Access control risks, vulnerabilities, and exposures

Security Architecture and Models

Secure operating system principles, concepts, mechanisms, controls, and standards
 Secure architecture design, modeling, and protection
 Security models: confidentiality, integrity, and information flow
 Government and commercial security requirements
 Common criteria, ITSEC, TCSEC, IETF, IPSEC
 Technical platforms
 System security preventative, detective, and corrective measures

Disaster Recovery and Business Continuity Planning

Business continuity planning, business impact analysis, recovery strategies, recovery plan development, and implementation
 Disaster recovery planning, implementation, and restoration
 Compare and contrast disaster recovery and business continuity

Security Management Practices

Organizational security roles
 Identification of information assets
 Security management planning
 Security policy development; use of guidelines, standards, and procedures
 Security awareness training
 Data classification and marking
 Employment agreements and practices
 Risk management tools and techniques

Law, Investigation, and Ethics

Computer crime detection methods
 Applicable computer crime, security, and privacy laws
 Evidence gathering and preservation methods
 Computer crime investigation methods and techniques
 Civil, criminal, and investigative law
 Intellectual property law
 ISC2 and IAB ethics application

Physical Security

Prevention, detection, and correction of physical hazards
 Secure site design, configuration, and selection elements
 Access control and protection methods for facility, information, equipment, and personnel

Operations Security

Resource protection mechanisms and techniques
 Operation security principles, techniques, and mechanisms; principles of good practice and limitation of abuses

Operations security preventative, detective, and corrective measures
 Information attacks
 Access Control Subversion

Cryptography

Cryptographic concepts, methods, and practices
 Construction of algorithms
 Attacks on cryptosystems
 Ancient cryptography and modern methods
 Public and private key algorithms and uses
 Key distribution and key management
 Digital signature construction and use
 Methods of attack, strength of function

Telecommunications and Network Security

Overview of communications and network security
 Voice communications, data communications, local area, wide area, and remote access
 Internet/Intranet/Extranet, firewalls, routers, and network protocols
 Telecommunication and network security preventative, detective, and corrective measures
 System development process and security controls
 System development life cycle, change controls, application controls, and system and application integrity
 Database structure, concepts, design techniques, and security implications
 Object oriented programming
 Data warehousing and data mining

Review and Q&A Session

Review concepts introduced in previous sessions
 Answer specific questions or concerns regarding CISSP preparation material

Testing-Taking Tips and Study Techniques

Tips for additional preparation for the CISSP exam
 Additional resources
 Techniques for scoring well on the exam