CISSP

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.

Course Outline:

Access Control Systems and Methodologies

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

Security Architecture and Models

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

Disaster Recovery and Business Continuity Planning

1. Business continuity planning, business impact analysis, recovery strategies, recovery plan
2. development, and implementation
3. Disaster recovery planning, implementation, and restoration
4. Compare and contrast disaster recovery and business continuity

Security Management Practices

1. Organizational security roles
2. Identification of information assets
3. Security management planning
4. Security policy development; use of guidelines, standards, and procedures
5. Security awareness training
6. Data classification and marking
7. Employment agreements and practices
8. Risk management tools and techniques

Law, Investigation, and Ethics

1. Computer crime detection methods
2. Applicable computer crime, security, and privacy laws
3. Evidence gathering and preservation methods
4. Computer crime investigation methods and techniques
5. Civil, criminal, and investigative law
6. Intellectual property law
7. ISC2 and IAB ethics application

Physical Security

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

Operations Security

1. Resource protection mechanisms and techniques
2. Operation security principles, techniques, and mechanisms; principles of good practice and
3. limitation of abuses
4. Operations security preventative, detective, and corrective measures
5. Information attacks
6. Access Control Subversion

Cryptography

1. Cryptographic concepts, methods, and practices
2. Construction of algorithms
3. Attacks on cryptosystems
4. Ancient cryptography and modern methods
5. Public and private key algorithms and uses
6. Key distribution and key management
7. Digital signature construction and use
8. Methods of attack, strength of function

Telecommunications and Network Security

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

Review and Q&A Session

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

Testing-Taking Tips and Study Techniques

1. Tips for additional preparation for the CISSP exam
2. Additional resources
3. Techniques for scoring well on the exam


CORPORATION
LEARNING ALLIANCE