CISSP Certification Preparation

Duration: 5 Days   Course Code: 9840   Delivery Method: Virtual and Classroom

Overview:

If you are ready to take your security career to the next level, our Certified Information Systems Security Professional (CISSP) exam preparation course will help get you there. Get instruction from our experts with real-world experience as you cover all the material you need to be fully prepared for the (ISC)2 CISSP exam. Delegates will receive a copy of the CISSP (ISC)2 Certified Information Systems Security Professional Officieal Study Guide (Seventh Edition).

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Sense IT will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

IT consultants, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, security engineers, and other security professionals whose positions require CISSP certification.

Objectives:

- At the end of this course delegates will be able to;
- In-depth coverage of the eight domains required to pass the CISSP exam:
- Security and Risk Management
- Asset Security
- Security Engineering and Cryptography
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Security in the Software Development Lifecycle

Prerequisites:

Follow-on-Courses:

You must have a minimum of five years of direct full-time security work experience in two or more of these 8 domains of the (ISC)^2 CISSP CBK:

- Security and Risk Management (Security, Risk, Compliance, Law, Regulations, and Business Continuity)
- Asset Security (Protecting Security of Assets)
- Security Engineering (Engineering and Management of Security)
- Communication and Network Security (Designing and Protecting Network Security)
- Identity and Access Management (Controlling Access and Managing Identity)
- Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
- Security Operations (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)
- Software Development Security (Understanding, Applying, and Enforcing Software Security)

Students attending this course may wish to further expand their knowledge in specific areas by attending Wireless Networking or Network Security Courses.

Content:

Test-Taking Tips and Study Techniques

- Preparation for the CISSP Exam
- Submitting Required Paperwork
- Resources and Study Aids
- Passing the Exam the First Time

Security and Risk Management (Security, Risk, Compliance, Law, Regulations, and Business Continuity)

- Confidentiality, integrity, and availability concepts
- Security governance principles
- Compliance
- Legal and regulatory issues
- Professional ethic
- Security policies, standards, procedures and guidelines

Asset Security (Protecting Security of Assets)

- Information and asset classification
- Ownership (e.g. data owners, system owners)
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements (e.g. markings, labels, storage)

Security Engineering (Engineering and Management of Security)

- Engineering processes using secure design principles
- Security models fundamental concepts
- Security evaluation models
- Security capabilities of information systems
- Security architectures, designs, and solution elements vulnerabilities
- Web-based systems vulnerabilities
- Mobile systems vulnerabilities
- Embedded devices and cyber-physical systems vulnerabilities
- Cryptography
- Site and facility design secure principles
- Physical security

Communication and Network Security (Designing and Protecting Network Security)

- Secure network architecture design (e.g. IP ; non-IP protocols, segmentation)
- Secure network components
- Secure communication channels
- Network attacks

Identity and Access Management (Controlling Access and Managing Identity)

- Physical and logical assets control
- Identification and authentication of people and devices
- Identity as a service (e.g. cloud identity)
- Third-party identity services (e.g. on-premise)
- Access control attacks
- Identity and access provisioning lifecycle (e.g. provisioning review)

Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)

- Assessment and test strategies
- Security process data (e.g. management and operational controls)
- Security control testing
- Test outputs (e.g. automated, manual)
- Security architectures vulnerabilities

Security Operations (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)

- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

Software Development Security (Understanding, Applying, and Enforcing Software Security)

- Security in the software development lifecycle
- Development environment security controls
- Software security effectiveness
- Acquired software security impact

Review and Q;A Session

- Final Review and Test Prep