CISSP Certification Prep Course v1.0

Duration: 5 Days Course Code: GK9803

Overview:

Gain core knowledge and experience to successfully implement and manage security programs and prepare for the CISSP certification. This course is the most comprehensive review of information security concepts and industry best practices, and focuses on the eight domains of the CISSP CBK (Common Body of Knowledge) that are covered in the CISSP exam. You will gain knowledge in information security that will increase your ability to successfully implement and manage security programs in any organization or government entity.
Why take the CISSP Certification Prep Course?
The CISSP exam is challenging, but the benefits are immense. Due to its comprehensive breadth, CISSP is the de facto certification to show competence in cyber roles. It is also one of the top-paying certifications in IT.
This course supports a certification that is a DoD Approved 8570 Baseline Certification and meets DoD 8140/8570 training requirements.

Target Audience:

Individuals looking to establish information security best practices within their organisations or those looking to advance their career within the information security arena.

Objectives:

- After completing this course you should have an in-depth understanding of the eight fundamental domains of information security:
- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Prerequisites:

Attendees should meet the following prerequsites:

- A minimum of 5 years' experience working in IT infrastructure and Cybersecurity

Testing and Certification

Recommended as preparation for the following exams:

- CISSP – Certified Information Systems Security Professional

To qualify for this cybersecurity certification, you must pass the exam and have at least five years of cumulative, paid work experience in two or more of the eight domains of the (ISC)² CISSP Common Body of Knowledge (CBK).

It may be possible to satisfy one year of required work experience with a relevant four-year college degree or if you hold an approved credential.

Even if you don't have the required level of experience you can still pass the CISSP exam and become an Associate of (ISC)² while you earn the required work experience.

Content:

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

- Understand and Apply Concepts of Confidentiality, Integrity, and Availability
- Apply Security Governance Principles
- Compliance
- Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context
- Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines
- Understand Business Continuity Requirements
- Contribute to Personnel Security Policies
- Understand and Apply Risk Management Concepts
- Understand and Apply Threat Modeling
- Integrate Security Risk Considerations into Acquisitions Strategy and Practice
- Establish and Manage Security Education, Training, and Awareness

Asset Security (Protecting Security of Assets)

- Classify Information and Supporting Assets
- Determine and Maintain Ownership
- Protect Privacy
- Ensure Appropriate Retention
- Determine Data Security Controls
- Establish Handling Requirements

Security Engineering (Engineering and Management of Security)

- Implement and Manage an Engineering Life Cycle Using Security Design Principles
- Understand Fundamental Concepts of Security Models
- Select Controls and Countermeasures Based Upon Information Systems Security Standards
- Understand the Security Capabilities of Information Systems
- Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements
- Assess and Mitigate Vulnerabilities in Web-based Systems
- Assess and Mitigate Vulnerabilities in Mobile Systems
- Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems
- Apply Cryptography
- Apply Secure Principles to Site and Facility Design
- Design and Implement Facility Security

Communications and Network Security (Designing and Protecting Network Security)

- Apply Secure Design Principles to Network Architecture
- Securing Network Components
- Design and Establish Secure Communication Channels
- Prevent or Mitigate Network Attacks

Identity and Access Management (Controlling Access and Managing Identity)

- Control Physical and Logical Access to Assets
- Manage Identification and Authentication of People and Devices
- Integrate Identity as a Service (IDaaS)
- Integrate Third-Party Identity Services
- Implement and Manage Authorization Mechanisms
- Prevent or Mitigate Access Control Attacks
- Manage the Identity and Access Provisioning Life Cycle

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

- Design and Validate Assessment and Test Strategies
- Conduct Security Control Testing
- Collect Security Process Data
- Conduct or Facilitate Internal and Third-Party Audits

Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

- Understand and Support Investigations
- Understand Requirements for Investigation Types
- Conduct Logging and Monitoring Activities
- Secure the Provisioning of Resources through Configuration Management
- Understand and Apply Foundational Security Operations Concepts
- Employ Resource Protection Techniques
- Conduct Incident Response
- Operate and Maintain Preventative Measures
- Implement and Support Patch and Vulnerability Management
- Participate in and Understand Change Management Processes
- Implement Recovery Strategies
- Implement Disaster Recovery Processes
- Test Disaster Recovery Plan
- Participate in Business Continuity Planning
- Implement and Manage Physical Security
- Participate in Personnel Safety

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

- Understand and Apply Security in the Software Development Life Cycle
- Enforce Security Controls in the Development Environment
- Assess the Effectiveness of Software Security

Assess Software Acquisition Security

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo