CISSP-Certified Information Systems Security Professional - Certification Preparation

Duration: 5 Days **Course Code: GK9803**

Overview:

The CISSP - Certified Information Systems Security Professional- certificate gives you international recognition as a security professional from ISC2. This training prepares you for the CISSP exam of ISC2.

Target Audience:

The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the following positions: Chief Information Security OfficerChief Information OfficerDirector of SecurityIT Director/ManagerSecurity Systems EngineerSecurity AnalystSecurity ManagerSecurity AuditorSecurity ArchitectSecurity ConsultantNetwork Architect

Objectives:

- This course is a comprehensive and compact review of the eight domains of the official CISSP CBK (Common Body of Knowledge). 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. Policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets are also covered in this course.
- The CISSP CBK covers the following domains:
- Security and Risk Management
- Asset Security
- Security Engineering
- Communications & Network Security
- Identity & Access Management
- Security Assessment & Testing
- Security Operations
- Software Development Security
- This five-day program is comprised of a total of eight domains and includes:
- Official (ISC)2 Guide to the CISSP Common Body of Knowledge® (CBK)
- Additional CISSP Study Guide
- Additional Study material
- Delegates who would like to succesfully pass the CISSP exam are advised to self-study the 8 domains after attendance.

Prerequisites:

Professionals with at least five years of experience and who demonstrate a globally recognized level of competence, as defined in the CISSP Common Body of Knowledge (CBK) in two or more of the eight security domains.

- 9701 - Cybersecurity Foundations
- G013 - CompTIA Security+ (SY0-601)

Testing and Certification

- This course prepares you for the ISC(2) CISSP examination.
- The examination itself is not part of this course.
- We recommend taking the exam soon after completing the course. Please plan on doing some self-study to prepare for the exam, you can also leverage the practice questions that will be supplied at the start of the course to assess your readiness level. We recommend reserving at least 2 weeks after the course so your exam preparation can fit in with your regular workload/hours.

Follow-on-Courses:

- GK1642 - SSCP-Systems Security Certified Practitioner) - Certification Preperation

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 AwarenessAsset 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 RequirementsSecurity 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 SecurityCommunications 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 AttacksIdentity 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 CycleSecurity 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 AuditsSecurity 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 SafetySoftware 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 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/