CISSP-Certified Information Systems Security Professional - Certification Preparation

Duration: 5 Days Course Code: GK9803 Delivery Method: Company Event

Overview:

Gain core knowledge and experience to successfully implement and manage security programs and prepare for the 2022 CISSP certification.
This 2022 updated course is the most comprehensive review of information security concepts and industry best practices, focusing 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.
In addition to a textbook, you will receive practice test questions with complete answer explanations and flashcards to help you prepare for certification.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

Anyone whose position requires CISSP certification Individuals who want to advance within their current computer security careers or migrate to a related career

Objectives:

- This course provides in-depth coverage of the eight domains required to pass the CISSP exam:
- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security
- 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's 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.**
- Global Knowledge is independent of and not affiliated with (ISC)2.

Prerequisites:

To be successful in this course, you should have a minimum of five years of experience working in IT Infrastructure and Cybersecurity.

- Cybersecurity Foundations
- CompTIA Security+ Certification Prep Course
- Cybersecurity Specialization: Architecture and Policy
- Cybersecurity Specialization: Governance, Risk, and Compliance
- 9701 - Cybersecurity Foundations
- G013 - CompTIA Security+

Testing and Certification

CISSP - Certified Information Systems Security Professional

Follow-on-Courses:

- SSCP Certification Prep Course
- CCSP Certification Prep Course
- GK1642 - SSCP-Systems Security Certified Practitioner - Certification Preperation

Content:

1: Security Governance Through Principles and Policies

- Security 101
- Understand and Apply Security Concepts
- Security Boundaries
- Evaluate and Apply Security Governance Principles
- Manage the Security Function
- Security Policy, Standards, Procedures, and Guidelines
- Threat Modeling
- Supply Chain Risk Management

2: Personnel Security and Risk Management Concepts

- Personnel Security Policies and Procedures
- Understand and Apply Risk Management Concepts
- Social Engineering
- Establish and Maintain a Security Awareness, Education, and Training Program

3: Business Continuity Planning

- Planning for Business Continuity
- Project Scope and Planning
- Business Impact Analysis
- Continuity Planning
- Plan Approval and Implementation

4: Laws, Regulations, and Compliance

- Categories of Laws
- Laws
- State Privacy Laws
- Compliance
- Contracting and Procurement

5: Protecting Security of Assets

- Identifying and Classifying Information and Assets
- Establishing Information and Asset Handling Requirements
- Data Protection Methods
- Understanding Data Roles
- Using Security Baselines

6: Cryptography and Symmetric Key Algorithms

- Cryptographic Foundations
- Modern Cryptography
- Symmetric Cryptography
- Cryptographic Lifecycle

7: PKI and Cryptographic Applications

- Asymmetric Cryptography
- Hash Functions
- Digital Signatures

8: Principles of Security Models, Design, and Capabilities

- Secure Design Principles
- Techniques for Ensuring CIA
- Understand the Fundamental Concepts of Security Models
- Select Controls Based on Systems Security Requirements
- Understand Security Capabilities of Information Systems

9: Security Vulnerabilities, Threats, and Countermeasures

- Shared Responsibility
- Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements
- Client-Based Systems
- Server-Based Systems
- Industrial Control Systems
- Distributed Systems
- High-Performance Computing (HPC) Systems
- Internet of Things
- Edge and Fog Computing
- Embedded Devices and Cyber-Physical Systems
- Specialized Devices
- Microservices
- Infrastructure as Code
- Virtualized Systems
- Containerization
- Serverless Architecture
- Mobile Devices
- Essential Security Protection Mechanisms
- Common Security Architecture Flaws and Issues

10: Physical Security Requirements

- Apply Security Principles to Site and Facility Design
- Implement Site and Facility Security Controls
- Implement and Manage Physical Security

11: Secure Network Architecture and Components

- OSI Model
- TCP/IP Model
- Analyzing Network Traffic
- Common Application Layer Protocols
- Transport Layer Protocols
- Domain Name System
- Internet Protocol (IP) Networking
- ARP Concerns
- Secure Communication Protocols
- Implications of Multilayer Protocols
- Microsegmentation

15: Security Assessment and Testing

- Building a Security Assessment and Testing Program
- Performing Vulnerability Assessments
- Testing Your Software
- Implementing Security Management Processes

16: Managing Security Operations

- Apply Foundational Security Operations Concepts
- Addressing Personnel Safety and Security
- Provision Resources Securely
- Apply Resource Protection
- Managed Services in the Cloud
- Perform Configuration Management (CM)
- Managing Change
- Managing Patches and Reducing Vulnerabilities

17: Preventing and Responding to Incidents

- Conducting Incident Management
- Implementing Detective and Preventive Measures
- Logging and Monitoring
- Automating Incident Response

18: Disaster Recovery Planning

- The Nature of Disaster
- Understand System Resilience, High Availability, and Fault Tolerance
- Recovery Strategy
- Recovery Plan Development
- Training, Awareness, and Documentation
- Testing and Maintenance

19: Investigations and Ethics

- Investigations
- Major Categories of Computer Crime
- Ethics

20: Software Development Security

- Introducing Systems Development Controls
- Establishing Databases and Data Warehousing
- Storage Threats
- Understanding Knowledge-Based Systems

21: Malicious Code and Application Attacks

- Malware
- Malware Prevention
- Application Attacks
- Injection Vulnerabilities
- Exploiting Authorization Vulnerabilities
- Exploiting Web Application Vulnerabilities

- Public Key Infrastructure
- Asymmetric Key Management
- Hybrid Cryptography
- Applied Cryptography
- Cryptographic Attacks

- Wireless Networks
- Other Communication Protocols
- Cellular Networks
- Content Distribution Networks (CDNs)
- Secure Network Components

12: Secure Communications and Network Attacks

- Protocol Security Mechanisms
- Secure Voice Communications
- Remote Access Security Management
- Multimedia Collaboration
- Load Balancing
- Manage Email Security
- Virtual Private Network
- Switching and Virtual LANs
- Network Address Translation
- Third-Party Connectivity
- Switching Technologies
- WAN Technologies
- Fiber-Optic Links
- Security Control Characteristics
- Prevent or Mitigate Network Attacks

13: Managing Identity and Authentication

- Controlling Access to Assets
- Managing Identification and Authentication
- Implementing Identity Management
- Managing the Identity and Access Provisioning Lifecycle

14: Controlling and Monitoring Access

- Comparing Access Control Models
- Implementing Authentication Systems
- Understanding Access Control Attacks

- Application Security Controls
- Secure Coding Practices

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK