CISSP-Certified Information Systems Security Professional - Certification Preparation

Duration: 5 Days **Course Code: GK9803** **Delivery Method: Virtual Learning**

Overview:

Gain core knowledge and experience to successfully implement and manage security programs and prepare for the 2024 CISSP certification.

This 2024 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 also receive access to Sybex's online interactive learning environment that includes:
- Over 900 practice test questions with complete answer explanations.
- More than 1000 Electronic Flashcards
- A searchable glossary in PDF to give you instant access to the key terms you need to know

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, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

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 Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Prerequisites:

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

- 9701 - Cybersecurity Foundations
- G013 - CompTIA Security+

Testing and Certification

- This course prepares you for the 2024 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:

Chapter 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

Chapter 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

Chapter 3 Business Continuity Planning

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

Chapter 4 Laws, Regulations, and Compliance

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

Chapter 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

Chapter 6 Cryptography and Symmetric Key Algorithms

- Cryptographic Foundations
- Modern Cryptography
- Symmetric Cryptography
- Cryptographic Life Cycle

Chapter 7 PKI and Cryptographic Applications

- Asymmetric Cryptography
- Hash Functions

Chapter 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

Chapter 9 Security Vulnerabilities, Threats, and Countermeasures

- Shared Responsibility
- Data Localization and Data Sovereignty
- 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
- Real-Time Operating Systems
- Internet of Things
- Edge and Fog Computing
- Embedded Devices and Cyber-Physical Systems
- Microservices
- Infrastructure as Code
- Immutable Architecture
- Virtualized Systems
- Containerization
- Mobile Devices
- Essential Security Protection Mechanisms
- Common Security Architecture Flaws and Issues

Chapter 10 Physical Security Requirements

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

Chapter 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
- Segmentation

Chapter 15 Security Assessment and Testing

- Building a Security Assessment and Testing Program
- Performing Vulnerability Assessments
- Testing Your Software
- Training and Exercises
- Implementing Security Management Processes and Collecting Security Process Data

Chapter 16 Managing Security Operations

- Apply Foundational Security Operations Concepts
- Address Personnel Safety and Security
- Provision Information and Assets Securely
- Managed Services in the Cloud
- Perform Configuration Management (CM)
- Manage Change
- Manage Patches and Reduce Vulnerabilities

Chapter 17 Preventing and Responding to Incidents

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

Chapter 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

Chapter 19 Investigations and Ethics

- Investigations
- Major Categories of Computer Crime
- Ethics

Chapter 20 Software Development Security

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

Chapter 21 Malicious Code and Application Attacks

- Malware
- Malware Prevention

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

- Edge Networks
- Wireless Networks
- Satellite Communications
- Cellular Networks
- Content Distribution Networks (CDNs)
- Secure Network Components

Chapter 12 Secure Communications and Network Attacks ·

- Protocol Security Mechanisms
- Secure Voice Communications
- Remote Access Security Management
- Multimedia Collaboration
- Monitoring and Management
- 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
- Prevent or Mitigate Network Attacks

Chapter 13 Managing Identity and Authentication

- Controlling Access to Assets
- The AAA Model
- Implementing Identity Management
- Managing the Identity and Access Provisioning Life Cycle

Chapter 14 Controlling and Monitoring Access

- Comparing Access Control Models
- Implementing Authentication Systems
- Zero-Trust Access Policy Enforcement
- Understanding Access Control Attacks

- Application Attacks
- Injection Vulnerabilities
- Exploiting Authorization Vulnerabilities
- Exploiting Web Application Vulnerabilities
- Application Security Controls
- Secure Coding Practices

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