Official ISC2 Certified Information Systems Security Professional Training (CISSP)

Duration: 5 Days **Course Code: CISSP**

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

Updated August 2026

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 2026 ISC2 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:

- SSCP - Official ISC2 Systems Security Certified Practitioner (SSCP) Training

Content:

Module 1: Security and Risk Management

- Understand, adhere to, and promote professional ethics
- Understand and apply security concepts
- Evaluate and apply security governance principles
- Determine compliance and other requirements
- Understand legal and regulatory issues that pertain to information security in a holistic context
- Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modeling concepts and methodologies
- Apply Supply Chain Risk Management (SCRM) concepts
- Establish and maintain a security awareness, education, and training program

Module 2: Asset Security

- Identify and classify information and assets
- Establish information and asset handling requirements
- Provision resources securely
- Manage data lifecycle
- Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))
- Determine data security controls and compliance requirements

Module 3: Security Architecture and Engineering

- Research, implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)
- Select controls based upon systems security requirements
- Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Select and determine cryptographic solutions

Module 4: Communication and Network Security

- Assess and implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

Module 5: Identity and Access Management (IAM)

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Federated identity with a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle
- Implement authentication systems

Module 6: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate a report
- Conduct or facilitate security audits

Module 7: Security Operations

- Understand and comply with investigations
- Conduct logging and monitoring activities
- Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
- Apply foundational security operations concepts
- Apply resource protection
- Conduct incident management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

Module 8: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in software development ecosystems
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure code

- Understand methods of cryptanalytic attacks
- Apply security principles to site and facility design
- Design site and facility security controls

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE