CISSP®

Certified Information Systems Security Professional

Duration: 5 Days

The ISC(2) CISSP Certified Information Systems Security Professional Certification is one of the most sought-after security certifications available today. It is based on the CBK (Common Body of Knowledge) which comprises eight subject domains that the (ISC)2 compiles and maintains through ongoing peer review by subject matter experts.

This 5-day accelerated course provides information security professionals with a fully-immersed, minimum-distraction CISSP training and certification experience.

The course will broaden and deepen your understanding of the CBK domains and give you full preparation for the (ISC)2 CISSP accreditation examination.

Who Should Attend

This course is designed for experienced security professionals who want to expand their knowledge and gain an internationally recognised accreditation.

Whilst anyone can attend the course, please note that the CISSP accreditation is only available to those who meet the (ISC)2 entry requirements.

Learning Outcomes

This program is designed to fully prepare you for the CISSP exam. Course attendees learn in detail about the ten domains covered under the (ISC)2 Common Body of Knowledge (CBK), including an understanding of the related concepts, skill sets and technologies used to plan for, design, and manage each domain.

1. Security and Risk Management
2. Security Engineering
3. Security Assessment and Testing
4. Asset Security
5. Communications and Network Security
6. Identity and Access Management
7. Security in the Software Development Life Cycle
8. Security Operations

Prerequisites

The course assumes you have varied IT experience gained over a number of years. Please note that in order to be eligible to sit for the CISSP exam you must have either five years of experience in Information or Computer Security.

Examination Procedure

The CISSP exams are administered by Pearson Vue on behalf of (ISC)2. You must register for the exam online. For information on dates or how to enrol for an exam please contact ALC.

Course Contents

1. Security and Risk Management
- Security Properties of Information and Systems – The CIA Triad
- Security Governance

2. Security Engineering
- Security Engineering Lifecycle
- Systems Architecture
- Enterprise Security Architecture
- Security Models

3. Security Assessment and Testing
- Security Audit, Assessment and Testing Concepts
- Software Security Assessment
- Systems Security Assessment

4. Asset Security
- Information Assets – Identification, Ownership
- Data Standards and Policy
- Information Classification

5. Communications and Network Security
- Networking Principles
- Physical Layer
- Network Layer
- Transport Layer
- Application Layer

6. Identity and Access Management
- Basic Concepts: Trust, Identity, Authentication and Access Control
- Authentication Techniques

7. Security in the Software Development Life Cycle
- Application Development Concepts
- Vulnerabilities Introduced During Development
- Software Development

8. Security Operations
- Security Operations and Operations Security
- Threats and Vulnerabilities
- Viruses, Worms, Trojans, etc.

Refer to our website for more detailed information on the 8 CISSP domains

Get ahead of the game.
Get certified.
www.alcgroup.com