CISSP® Certified Information Systems Security Professional

Intensive 5 day course providing full preparation for the CISSP exam

Duration: 5 days

This 5-day concentrated course provides information security professionals with a fully-immersed, minimum-distraction CISSP training and certification experience. The course covers the 8 domains of the CISSP Common Body of Knowledge as reorganised in early 2015 and fully includes the updates that came into effect from 1 April 2018.

CISSP is long regarded as the gold standard of security qualifications. It draws from a comprehensive, up-to-date, global common body of knowledge that ensures security leaders have a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices.

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.

Prerequisites

The course assumes you have at least a reasonable level of varied IT experience. Please note that to attain the CISSP certification you must have a minimum of 5 years of direct, full-time security professional work experience in 2 or more of the domains of the CISSP CBK. One year of work experience may be waived by (ISC)2 if you hold a four-year or higher college or university degree or approved credential. Candidates who do not meet these criteria may be given Associate status until conditions are met.

Who Should Attend

The CISSP is designed for experienced security professionals who want to expand their knowledge and gain an internationally recognised accreditation. It is ideal for those working in positions such as: Security Consultant, Security Manager, IT Director/Manager, Security Auditor, Security Architect, Security Analyst, Security Systems Engineer, Chief InfoSec Officer, Director of Security, Network Architect.

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. Introduction

- Review and Revision Techniques
- References
- Specialised References and Additional Reading
- The “CISSP World-View”

2. Security & Risk Management

- Security Properties of Information and Systems – The CIA Triad
- Security Governance
- Compliance, Legal and Regulatory Requirements
- Risk Management Concepts

3. Security Engineering

- Security Engineering Lifecycle
- Systems Architecture
- Enterprise Security Architecture
- Security Models
- Evaluation, Certification and Accreditation
- Security Implementation Guidelines, Frameworks and Standards
- Database Security
- Vulnerabilities
- Cryptology
- Site Planning and Design
- Facility Security

4. Security Assessment & Testing

- I Security Audit, Assessment and Testing Concepts
- Software & Systems Sec. Assessment
- Network Security Assessment

5. Asset Security

- Information Assets – ID, Ownership
- Data Standards and Policy
- Information Classification
- Handling Requirements
- Data Retention Policy, Destruction and Disposal

6. Comms. & Network Security

- Networking Principles
- Physical & Network Layer
- Transport Layer
- Application Layer

7. Identity & Access Management

- Basic Concepts: Trust, Identity, Authentication and Access Control
- Authentication Techniques
- Authorization and Access Control
- Federated Identity Management Systems
- Identity Management Lifecycle

8. Security in the Software Development Life Cycle

- Application Development Concepts
- Vulnerabilities Introduced During Development
- Software Development Methodologies
- Databases and Data Warehouses
- Web Application Security

9. Security Operations

- Security Operations and Operations Security
- Threats and Vulnerabilities
- Configuration and Change Management
- Patch Management and Vulnerabilities
- Security Metrics, Monitoring and Reporting
- Incident Response