Course Outline

ADVANCEDTRAINING
Inspire. Grow. Achieve.

CISSP- Certified Information Systems Security Professional

General Description

Our Certified Information Systems Security Professional (CISSP) training course aims to supply delegates with a theory-based approach to learning the Information Systems security process and how to apply this process practically to real-life scenarios. The course is based around teaching the eight fundamental domains of Information Security, which provide delegates with all the information they require to obtain a broad understanding of Information Security and pass the CISSP exam.
The CISSP certification is globally recognised as the best Information Systems Security certification for Security Professionals. Our trainers use a theory-based training strategy, allowing for a clear explanation of CISSP terminology and methodology.

Audience Profile

This CISSP training course is suitable for mid- and senior-level managers who are working towards or have already achieved a position such as:

- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)
- Senior Security Engineer
- Security Consultant
- Security Manager
- Security Auditor
- Security Architect
- Network Architect

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

What is included

This CISSP course will include:

- Exam Pass Guarantee
- Certificate
- Experienced Instructor

Microsoft Partner
Silver Learning

Prerequisites

No prior certifications are required, but delegates will thrive if they possess experience or knowledge of IS Security

Course Details

Course code: CISSP
Duration: 5 days
Starting time: 9am
Finishing time: 4.30pm

Booking guidelines

Contact our learning consultants on 1300 86 87246 and we will assist you with your booking.

☎ 1300 86 87246
1300 TO TRAIN

Course Outline

ADVANCEDTRAINING
Inspire. Grow. Achieve.

1. Introduction

- Welcome and Administrivia
- Course Overview
- Review and Revision Techniques
- References
- Specialised References and Additional Reading
- Other Resources
- The "CISSP World-View"
- The Exam
- On the Day of the Exam
- Exam Technique
- After the Exam
- CISSP Concentrations
- Blended Learning Follow-up

The following subjects will be taught during this five-day CISSP course:

Security and Risk Management:

- Confidentiality, Integrity, and Availability Concepts
- Security Governance Principles
- Compliance
- Legal and Regulatory Issues
- Professional Ethics
- Security Policies, Standards, Procedures, and Guidelines

Asset Security:

- Information and Asset Classification
- Ownership
- Protect Privacy
- Appropriate Retention
- Data Security Controls
- Handling Requirements

Security Architecture and Engineering:

- Engineering Processes using Secure Design Principles
- Security Models Fundamental Concepts
- Security Evaluation Models
- Security Capabilities of Information Systems
- Security Architectures, Designs, and Solution Elements Vulnerabilities
- Web-based Systems Vulnerabilities
- Mobile Systems Vulnerabilities
- Embedded Devices and Cyber-Physical Systems Vulnerabilities
- Cryptography
- Site and Facility Design Secure Principles
- Physical Security

Communication and Network Security:

- Secure Network Architecture Design
- Secure Network Components
- Secure Communication Channels
- Network Attacks

Identity and Access Management (IAM):

- Physical and Logical Assets Control
- Identification and Authentication of People and Devices
- Identity as a Service
- Third-party Identity Services
- Access Control Attacks
- Identity and Access Provisioning Lifecycle

Security Assessment and Testing:

- Assessment and Test Strategies
- Security Process Data
- Security Control Testing
- Test Outputs
- Security Architectures Vulnerabilities

Security Operations:

- Investigations Support and Requirements
- Logging and Monitoring Activities
- Provisioning of Resources
- Foundational Security Operations Concepts
- Resource Protection Techniques
- Incident Management
- Preventative Measures
- Patch and Vulnerability Management
- Change Management Processes
- Recovery Strategies
- Disaster Recovery Processes and Plans
- Business Continuity Planning and Exercises
- Physical Security
- Personnel Safety Concerns

Software Development Security:

- Security in the Software Development Lifecycle
- Development Environment Security Controls
- Software Security Effectiveness
- Acquired Software Security Impact

Delegates should purchase the following book which will be used during the course: The Official (ISC)2 Guide to the CISSP CBK Reference, 5th Edition, by John Warsinske.

It might also prove useful to briefly read over some of this guide prior to starting the course to supplement your learning and prepare you for your CISSP training