Silicon Beach Training

follow us

Tel *+44(0)1273 6222 72*

www.siliconbeachtraining.co.uk

info@siliconbeachtraining.co.uk

CISSP Certified Information Systems Security Professional

Gain the knowledge to become an Information Systems Security Professional with our CISSP.

Our CISSP course lasts for 5 days and will help you succeed in a career of IS security. This course provides all the required knowledge to carry on and pass the CISSP exam.

Objective

Gain the knowledge to become an Information Systems Security Professional with our CISSP course.

Our CISSP course lasts for 5 days and will help you succeed in a career of IS security. This course provides all the required knowledge to carry on and pass the CISSP exam. This CISSP training course is the main way to show and exhibit your understanding of information security and what is required of a security professional.

Having previous experience with IS security for around 5 years is highly advised or 4 years plus an IS University degree. If you don't have this experience then you can become an Associate of $(ISC)^2$ which allows you to gain the necessary experience in the following 6 years instead.

Details

Duration: 5 Days

Who is this course for

There are no pre-requisites for this course.

Course Content

Security and Risk Management:

- Confidentiality, integrity, and availability concepts
- Security governance principles
- Compliance
- Legal and regulatory issues
- Professional ethic
- Security policies, standards, procedures and guidelines

Asset Security:

- Information and asset classification
- Ownership
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements

Security 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:

- 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

Silicon Beach Training Ltd

Moorgate House, 5-8 Dysart Street, London, EC2A 2BX