Silicon Beach Training

follow us

Tel *+44(0)1273 6222 72*

www.siliconbeachtraining.co.uk

info@siliconbeachtraining.co.uk

CISMP Training

Enhance your security management career with our BCS Certificate in Information Security Management Principles.

The CISMP qualification is a globally recognised certification which teaches you about information security management and the need for it.

Objective

By the end of completing the CISMP course delegates will:

- Gain knowledge on information security management
- Understand information security management regulations and legislation
- Gain awareness of the information security management national/international standards

Details

Duration: 5 Days

Who is this course for

There are no formal requirements for entry to the course.

Course Content

- The need for, and benefits of, information security: Corporate Governance.
- Information risk management.
- Information security organisation & responsibilities: Legal and regulatory obligations.
- Policies, standards & procedures: Delivering a balanced ISMS. Security procedures.
- Information security governance: Policy reviews. Security audits.
- Security incident management: Objectives and stages of incident management.
- Information security implementation: Getting management buy-in.
- Legal framework: Processing personal data. Employment issues. Computer misuse. Intellectual property rights. Data Protection Act.
- Security standards & procedures: ISO/IEC 27002 and ISO/IEC 15408.
- Threats to, and vulnerabilities of, information systems.
- People security: Organisational culture. Acceptable use policies.
- Systems development & support: Linking security to whole business process. Change management process. Handling security patches.
- Role of cryptography: Common encryption models.
- Protection from malicious software: Methods of control.
- User access controls: Authentication and authorisation mechanisms.
- Networks & communications: Partitioning networks. Role of cryptography. Controlling 3rd party access. Intrusion monitoring. Penetration testing, cloud computing.
- External services: Protection of Web servers and e-commerce applications.
- IT infrastructure: Operating, network, database and file management systems.
- Testing, audit & review: Strategies for security testing of business systems.
- Training: The purpose and role of training. Promoting awareness.
- Physical & environmental security: Controlling access and protecting physical sites and assets.
- Disaster recovery & business continuity management: Relationship between risk assessment and impact analysis.
- Investigations & forensics: Common processes, tools and techniques. Legal and regulatory guidelines.