



ISEB Certificate in Information Security Management Principles

Duration: 5 days

This intensive and highly practical 5-day course has been accredited by the Information Systems Examination Board (ISEB) of the British Computer Society (BCS). The course has been designed to provide the necessary information and guidance in order for delegates to be able to fulfil their roles as information security officers or information risk decision takers. It defines the business case for information security, the role of security as an enabler for business, and how to identify and manage information risks.

Delegates will be provided with a comprehensive understanding of the main concepts which underpin information security and how they relate to each other. The course covers such concepts as confidentiality, integrity and availability, threats, risks and vulnerabilities, as well as a range of technical and management controls capable of mitigating the risks.

The course examines current legislation and regulations which impact on information security as well as standards (ISO 17799 and ISO 27001) and frameworks which facilitate best practice.

The course will enable delegates to confidently sit the 2-hour multiple choice BCS/ISEB Certificate in Information Security Management Principles (CiISMP) exam which is taken on the final afternoon of the course.

Deliverables

On completion of this course delegates will:

- D be able to specify the business case for information security;
- D understand the challenges posed in managing information risk;
- D be able to address the business issues relating to legislation, regulation and corporate governance as it affects information security;
- D understand the issues and risks relating to information and have a clear insight into the controls needed to manage them;
- D understand how the different concepts of information security relate to each other;
- D be able to confidently sit the CiISMP exam.

Who should attend?

The course will benefit: any member of an information security management team; IT managers; security/systems administrators; internal auditors; staff with a local security co-ordination role; staff responsible for compliance with legislation and regulation relating to information technology, and corporate governance; staff working in business operational functions with responsibility for information assets and systems.

Pre-requisites

The recommended pre-requisite for attending this course and sitting the exam is a minimum of one year's experience in an IT function.

Benefits

By the end of this course, delegates will have a clear understanding of all the key components of information security best practice. Delegates will benefit from the practical experiences of URM's trainers who are all practising consultants and risk management experts. It is URM's policy that all trainers have real-life implementation and deployment experience within both public and private sector organisations which they can draw upon and share with course delegates. Each of URM's trainers holds a 'Pass-Distinction' in the CiSMP exam.

Course style

The CiSMP course is a mixture of traditional classroom training, syndicate exercises, mock exams and group discussions. Delegates are encouraged to participate throughout the course and are presented with draft policies and worked examples for discussion. There is a small amount of evening work which is mainly the revision of the comprehensive courseware notes. URM's consultants are on hand throughout the week, including the evenings, to answer delegates' questions and queries.

Course cost

Please contact 0118 902 7298,
info@ultimariskmanagement.com
www.ultimariskmanagement.com

Location

The training takes place at a dedicated training centre in Wyboston Lakes, Bedfordshire.

To register

For all enquiries, including dates, please contact 0118 902 7298,
info@ultimariskmanagement.com
www.ultimariskmanagement.com

Course topics

- D Information security concepts & definitions: Information Security Management System (ISMS) concept.
- D The need for, and benefits of, information security: Corporate Governance.
- D Information risk management.
- D Information security organisation & responsibilities: Legal and regulatory obligations.
- D Policies, standards & procedures: Delivering a balanced ISMS. Security procedures.
- D Information security governance: Policy reviews. Security audits.
- D Security incident management: Objectives and stages of incident management.
- D Information security implementation: Getting management buy-in.
- D Legal framework: Processing personal data. Employment issues. Computer misuse. Intellectual property rights. Data Protection Act.
- D Security standards & procedures: ISO/IEC 17799, ISO/IEC TR 13335 and ISO/IEC 27001.
- D Threats to, and vulnerabilities of, information systems.
- D People security: Organisational culture. Acceptable use policies.
- D Systems development & support: Linking security to whole business process. Change management process. Handling security patches.
- D Role of cryptography: Common encryption models.
- D Protection from malicious software: Methods of control.
- D User access controls: Authentication and authorisation mechanisms.
- D Networks & communications: Partitioning networks. Role of cryptography. Controlling 3rd-party access. Intrusion monitoring. Penetration testing.
- D External services: Protection of Web servers and e-commerce applications.
- D IT infrastructure: Operating, network, database and file management systems.
- D Testing, audit & review: Strategies for security testing of business systems.
- D Training: The purpose and role of training. Promoting awareness.
- D Physical & environmental security: Controlling access and protecting physical sites and assets.
- D Disaster recovery & business continuity management: Relationship between risk assessment and impact analysis.
- D Investigations & forensics: Common processes, tools and techniques. Legal and regulatory guidelines.

