Course Outline

Certificate in Information Security Management Principles (CISMP)

BCS Accredited 5 Day Course

OVERVIEW

This intensive and highly practical 5 day course has been accredited by BCS. The course has been designed to provide the necessary information and guidance in order for delegates to further their own understanding and improve organisational information security management arrangements.
The course will enable delegates to confidently sit the 2 hour multiple choice BCS Certificate in Information Security Management Principles (CISMP) exam which is taken on the final afternoon of the course. This CISMP course has been accredited as part of the CESG Certified Training (CCT) Scheme. The Scheme assesses cyber security training against relevant areas of the industry respected IISP Skills Framework and offers security professionals the opportunity to gain appropriate knowledge and skills.

WHO SHOULD ATTEND

The course will benefit those with an interest in information security, either as a potential career or as an additional part of their general business knowledge. It provides an ideal foundation on which other qualifications can be built. Delegates will be able to return to their organisation and contribute to the process of ensuring that information is appropriately protected.

PRE-REQUISITES

There are no pre-requisites for attending this course. However, delegates would benefit from having a general awareness of issues involved in managing information securely.

DELIVERABLES

On completion of this course delegates will:
• Be able to specify the business case for information security
• Understand the challenges posed in managing information risk including those of cyber security

• Be able to address the business issues relating to legislation, regulation and corporate governance as it affects information security
• Understand the issues and risks relating to information security management and have a clear insight into the controls needed to manage them
• Understand how the different concepts of information security management relate to each other
• Be able to confidently sit the CISMP exam.

BCS EXAMINATION

After taking the course, delegates will be able to sit a formal 2 hour examination set by BCS.
The examination comprises 100 multiple choice questions.
Students will need to obtain a mark of at least 65% to pass the examination and distinctions are awarded to candidates achieving a score of 80% or higher.

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.

COURSE TOPICS

• Information security concepts & definitions: Information Security Management System (ISMS) concept.
• The need for, and benefits of, information security: Corporate governance.
• Information risk management. • Information security organisation and responsibilities: Legal and regulatory obligations.
• Policies, standards and 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 and procedures: ISO 27000 series, ISO 15408, PCI DSS, PAS 555 and the Cyber Security Risk Governance and Management Specification.
• Threats to, and vulnerabilities of, information systems.
• People security: Organisational culture. Acceptable use policies.
• Systems development and 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 and communications: Partitioning networks. Role of cryptography. Controlling 3rd party access. Intrusion monitoring. Penetration testing. Cloud computing.
• IT infrastructure: Operating, network, database and file management systems.
• Testing, audit and review: Strategies for security testing of business systems.
• Training: The purpose and role of training. Promoting awareness.
• Physical and environmental security: Controlling access and protecting physical sites and other assets.
• Disaster recovery and business continuity management: Relationship between risk assessment and impact analysis.
• Investigations and forensics: Common processes, tools and techniques. Legal and regulatory guidelines.