Certificate in Information Security Management Principles

Why Attend

- The BCS Foundation Certificate in Information Security Management Principles (CISMP) is an entry-level information security course that is non-technical in nature. This 5-day course is designed to provide the knowledge and skills required to manage information security, information assurance and information risk-based processes.
- The CISMP qualification provides participants with detailed knowledge of the concepts relating to information security (confidentiality, integrity, availability, vulnerability, threats, risks and countermeasures), along with an understanding of current legislation and regulations which impact information security management. Certification holders will be able to apply the practical principles covered throughout the course to ensure their normal business processes become robust and more secure.
- The course follows the latest BCS syllabus and prepares participants for the multiple choice BCS examination which can be taken on the final day of the course, or remotely at a time of each participant's choice.

Course Methodology

- This course uses a mixture of presentations, videos, group discussions, individual research and quizzes.

Course Objectives

- Understand the current business and common technical environments in which information security must operate.
- Recognize current national and international standards, frameworks and organizations which facilitate the management of information security.
- Explain the fundamental concepts relating to information security management.
- Describe the categorization, operation and effectiveness of controls of different types and characteristics.
- Understand current legislation and regulations which impact upon information security management.

Target Audience

- This course is ideal for members of information security management teams, IT managers, security and systems managers, information asset owners and employees with legal compliance responsibilities.

Target Competencies

- Information security concepts
- Information security risk management
- Information security governance
- Business continuity management and disaster recovery
- Understanding of technical security controls

Information Security Management Principles

- Concepts and Definitions

Information Risk

- Threats
- Vulnerabilities
- Risk Management

Information Security Framework

- Organizations and responsibilities
- Organizational policy, standards, and procedures
- Information security governance
- Information assurance program implementation
- Security incident management
- Legal frameworks
- Security standards and procedures

Security Lifecycle

- The information life cycle
- Testing, audit, and review
- Systems development and support

Procedural / People Security Controls

- General controls
- People security
- User access controls
- Training and awareness

Technical Security Controls

- Technical security
- Protection from malicious software
- Networks and communications
- Operational Technology
- External services
- Cloud computing
- IT infrastructure

Physical and Environmental Security Controls

- Physical Security
- Different uses of controls

Disaster Recovery (DR) and Business Continuity Management (BCM)

- Relationship between DR/BCP, risk assessment and impact analysis
- Resilience and redundancy
- Approached to writing plans and implementing plans
- The need for documentation, maintenance, and testing
- The need for links to managed service provision and outsourcing
- The need for secure off-site storage of vital material
- The need to involve personnel, suppliers, and IT systems providers
- Relationship with security incident management
- Compliance with standards

Other Technical Aspects

- Investigations and forensics
- Role of cryptography
- Threat intelligence