Five Day – BCS Foundation Certificate in Information Security Management Principles

Maritemex
Holistic Cyber Security Resilience

1. COURSE

Upon completions, candidates will be able to demonstrate:

- Knowledge of the concepts relating to information security management
- Understanding of current national legislation and regulations which impact upon information security management
- Awareness of current national and international standards, frameworks and organisations which facilitate the management of information security
- Understanding of the current business and common technical environments in which information security management must operate
- Knowledge of the categorisation, operation and effectiveness of controls of different types and characteristics

2. MODULES OF THE CERTIFICATE WILL INCLUDE :

The CISMP course follows the latest BCS syllabus and covers the following areas:

- The need for information security
- Information Security Management System (ISMS) concepts and definitions
- Information risk management
- Corporate governance
- Organisational responsibilities
- Policies, standards and procedures
- Relevant ISO and IEC standards
- Information security controls
- Incident management
- The legal framework
- Cryptography
- Data communications and networks
- Physical security
- Security auditing
- Training and awareness
- Business continuity and disaster recovery
- Security investigations and forensics

3. COURSE CONTENT

The BCS Certificate in Information Security Management Principles (CISMP) course is designed to provide you with the knowledge and skills required to manage information security,

information assurance and information risk-based processes. It is aligned with the latest national information assurance frameworks (IAMM), as well as ISO/IEC 27002 & 27001; the code of practice and standard for information security.
The CISMP course follows the latest BCS syllabus and will prepare you for the BCS examination. This qualification provides you 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.

4. COURSE FORMAT

Learners will engage in an interactive workshop which will allow them to develop theoretical knowledge and apply it to their own situations. Delivery will be through a blended approach that will allow learners to fully engage in the session and gain practical examples of how to turn theory into practice.

5. DETAILED COURSE PROGRAM (unrolled training sequences)

Session 1 - Information Security Management Principles

- What security means
- The core concepts and definitions used in information security
- The key business drivers and how they shape the organization's approach to governance, risk management and compliance.
- The benefits of information security
- The role information security plays in an organization
- How an organization can make information security an integral part of its business.

Session 2 - Information Risk Management

- What risk means, how it arises and the likelihood of it impacting an organization.
- The effect big data, the Internet of Things and social media have on the risk landscape.
- Management techniques used by organizations to understand the risks they face
- Risk treatment and risk reduction methods
- The risk management lifecycle, illustrating how risks are identified, analysed, treated and

monitored
- Qualitative and quantitative methods of risk analysis
- How assets can be classified to help manage risk

Session 3 - Information Security Framework

- Where the security function fits within the organizational structure
- The role of the Information Security Officer
- Developing information security policies, standards and procedures
- The principles of information security governance
- How to carry out a security audit
- Implementing an information assurance programme and the importance of stakeholder engagement
- The incident management process and the role of digital forensics
- The legal information security framework
- Information assurance standards and how they should be applied within an organization

Session 4 - Procedural and People Security Controls

- The people threats facing organizations and the importance of a security culture
- Practical people controls, including employment contracts, service contracts, codes of conduct and acceptable use policies
- Access controls, including authentication and authorization, passwords, tokens and biometrics
- The importance of data ownership, privacy; access points, identification and authentication mechanisms, and information classification.
- How organizations can raise security awareness and the different approaches to deliver security-related training.

Session 5 - Technical Security Controls

- The different types of malware and the impact each one can have on an organization's
- computer systems
- Methods of accessing networks and how related security risks can be controlled
- The security issues related to networking services, including mobile computing, instant
- messaging and voice over IP
- Cloud computing deployment models and the security implications of cloud services
- The security requirements of an organization's IT infrastructure and the documentation
- required to support this.

Session 6 - Software Deployment and Lifecycle

- The software development lifecycle
- The role of testing and change control in reducing security related vulnerabilities in a production system
- How the risks introduced by third-party and outsourced developments can be mitigated

- Test strategies and test approaches, including vulnerability testing, penetration testing and code analysis
- The importance of reporting, and how reports should be structured and presented to stakeholders
- The principles of auditing and the role played by digital forensics.

Session 7 - Physical Security

- Physical, technical and procedural controls, including good environment design and
- premises security
- Clear screen and clear desk policies
- Reducing risks when moving property
- Securely disposing of property
- Maintaining security in delivery areas

Session 8 - Business Continuity and Disaster Recovery

- The value of business continuity management to an organization
- The business continuity management process
- The impact of business disruption on an organization and how long disruption should be
- tolerated
- The business continuity implementation process and implementation planning
- Disaster recovery strategy and the importance of disaster recovery planning
- Different standby systems and how these relate to recovery time
- The importance of robust documentation and testing of the plan.

Session 9 - Cryptography

- What cryptography is
- How cryptography works through symmetric ciphers, hash functions, asymmetric ciphers
- and digital
- signatures
- Key exchange and management
- Models of protection
- Cryptanalysis

5. COURSE PREPARATION

Although perceived as an Information Technology issue, information security is, in fact, a subject relevant to all business units. The CISMP course is relevant to anyone requiring an understanding of information security management as well as those with an interest in information security, either as a potential career, or as an additional part of their general business knowledge,

including members of information security management teams, IT managers, security and systems managers, information asset owners and employees with legal compliance responsibilities.

The course acts as a foundation for more advanced managerial or technical qualifications and provides a thorough general understanding to enable businesses to ensure their information is protected appropriately.
Prerequisites of the Certifications
There are no specific pre-requisites to study the CISMP course or for entry to the examination. However, the following knowledge would be advantageous:

- A basic knowledge of IT
- An understanding of the general principles of information technology security
- An awareness of the issues involved with security control activity

6. COURCE EVALUATION

Participant engagement and contribution is essential in this course. It is expected that all learners fully interact with the learning and the group activities.

7. BIOGRAPHY

Our experienced, expert and engaging NCSC and Executive Trainer pool includes the following profiles:

NCSC Certified and Executive Trainer: Experienced strategy adviser and solution Implementer, with international leadership experience in both government and commercial organisations. Over 22 years' experience in the fields of Cyber Security, Information Assurance and Information and Communications Technology after a background in Computer Science and Computing Information Systems. A Visiting Teacher of Cyber Security at the Oxford Martin School of Oxford University. Leads on audits and compliance-related activities with a focus on Critical National Infrastructure, including Central Government and Law Enforcement.

NCSC Certified Executive Trainer: Extensive financial services sector, developing Cyber Security and Information Assurance strategies, delivering Board briefings, leading audits and training and mentoring Senior Executives. Clients include G7 banks, central banks, retail banks and private equity firms. A thought leader in the area of Cyber Security and Information Assurance, speaking at conferences with articles regularly published. A visiting Professor at Oxford University.

NCSC Certified and Executive Trainer: Extensive experience includes mentoring Senior Executives in both the private and public sector. An established and highly effective leader with operational and commercial experience spanning private and defence sectors in the UK, Europe and the Middle East. Led Cyber Health Checks and Audits for multi-national clients, identifying key Cyber risks and threats and advising on improving Cyber resilience.

NCSC Certified and Executive Trainer: Expertise and experience in delivering training and workshops to Board and senior audiences across government and the commercial sector. Background includes geopolitical risk and global threats, information risk and security, as well as risk mitigation, crisis management and prevention. Fostered networks for sharing best practice with Cyber Security organisations in the US, the EU and across the Commonwealth and was a member of the Cyber Assessment Advisory Panel at the UK National Cyber Security Centre (NCSC).

NCSC Certified and Executive Trainer: coaches and trains leadership on Cyber and Risk across sectors and in the Critical National Infrastructure. Brings significant operational and field experience to his practitioner and academic work and specialises in the human dimension of cyber security. Previously, he was Chief Executive of a UK national body and author of a number of Cyber Security books sold internationally.

NCSC Certified and Executive Trainer: Experience of wide ranging oganisational support. Advises on information governance policy development and Cyber Security leadership and strategy. Background in education, academia and the not-for-profit sector has seen him advise government on national skills strategies and develop skills programmes in Cyber Security across the UK. Vice Chairman of the Information Assurance and Advisory Council. Working with national and regional bodies, and private sector parties, he focuses on developing regional cyber resilience strategy. Recipient of a National Cyber Security Award for his work with young people and cyber security.