Foundation Certificate in Information Security Management Principles (CISMP)

BCS Accredited Course

Deliverables

On completion of this course, you will be able to demonstrate knowledge and understanding of information security management principles in the following areas:

- Knowledge of the concepts relating to information security management (e.g. confidentiality, integrity, availability, vulnerability, threats, risks, countermeasures)
- Understanding of the relevant current legislation and regulations which impact upon information security management
- Comprehension of the relevant current national and international standards, frameworks and organisations which facilitate the management of information security
- Knowledge of the environments in which information security management has to operate
- Understanding of the categorisation, operation and effectiveness of controls of different types and characteristics

BCS Examination

After taking the course, you will be able to sit a 2 hour, closed-book examination set by BCS, comprising 100 multiple choice questions. You will need to obtain a mark of at least 65% to pass the examination

Benefits

By the end of this course, not only will you be in a position to pass the examination, but you will have a clear understanding of how the principles can be applied in your workplace. You will benefit, particularly, from the practical implementation experiences of URM's trainers who are all information security and risk management specialists.

Course Style

The CISMP course is a mixture of PowerPoint presentations, 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.

This intensive and highly practical course has been developed specifically against the BCS 2020 CISMP syllabus. By sitting this course, you will gain a unique insight into all aspects of information security and you will be able to return to your organisation and contribute to the process of ensuring that information is appropriately protected. URM's course will enable you to confidently sit the 2 hour multiple-choice BCS Foundation Certificate in Information Security Management Principles (CISMP) exam, which can be taken following the course. URM's CISMP course has been certified both by CIISec (the Chartered Institute of Information Security) and as part of the NCSC Certified Training scheme.

Who should attend?

The course will benefit anyone 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. It also provides the opportunity for those already working within information security to enhance or refresh their knowledge and in the process gain a qualification, recognised by industry, which demonstrates the level of knowledge gained.

Prerequisites

There are no specific prerequisites, although it would be helpful to have a working knowledge of IT and an understanding of the general principles of information technology security. However, by delivering the course over an extended period, rather than the 3 day BCS minimum, URM is providing more time to explain the fundamentals and explore the practical application of the various principles.

Comments from previous delegates

- I thoroughly enjoyed the course and most of that was down to the trainer's delivery of the course syllabus. The depth of general knowledge delivered by him on top of the detailed course material with reference to real world experience was outstanding. The course delivery exceeded my expectations and I am really pleased I went with URM as this course provider.
- The trainer was a great support throughout and couldn't have done more for us. The group size was just about right too and having the smaller group worked really well. The venue was great. All in all, I only have positive feedback and considered it a very positive experience thank you.
- The course was wonderful – very clear, easy to understand and very well planned. The venue was brilliant, I could not fault anything. On top of all that, the food was exceptional. I would not hesitate in recommending one of your courses and the venue. In fact, I am already looking into my next one as we speak!

Course Topics

Information Security Management Principles:

- **Definitions, meanings and use of concepts and terms**, inc. information security (confidentiality, integrity and availability); cyber security; asset types and valuation; risk management (threat, vulnerability, impact); risk appetite and tolerance; IS policy; IS controls; defence in depth and breadth; identity and AAA framework; accountability, audit and compliance; ethics; ISMS concept, assurance and governance.
- **Benefits of information security**, inc. protection of business assets; different business models and impact on security; changing environments; cost/impact vs risk reduction; role in overall security policy; relationship with corporate governance; security as an enabler.

Risk Management:

- **Threats to and vulnerabilities of information systems**, inc. threat intelligence and sharing; threat categorisation; accidental threats; deliberate threats; Dark Web; vulnerability categorisation; vulnerabilities of specific systems; impact assessment.
- **Processes for understanding and managing risk relating to information systems,** inc. 4 stage process; strategic options; tactical controls; operational controls; impact assessment (e.g. quantitative, qualitative); asset evaluation; information classification strategies; assessing risk in business terms; balancing IS costs against potential losses role of management; corporate risk registers.

Information Security Framework:

- **Implementing risk management in an organisation,** inc. organisations' management of information security; Organisational policy, standards and procedures; IS governance (e.g. audits, reviews, checks and reporting on compliance); IS implementation; security incident management.
- **Legal and regulatory compliance,** inc. protection of personal data; employment issues; computer misuse; records retention; intellectual property rights; contractual safeguards; admissible evidence; digital signatures; cryptography technology.
- **Common, established standards and procedures** inc. international standards (e.g. ISO 27001); product certification standards (e.g. ISO/IEC 15408); technical standards (e.g. NIST).

Security Lifecycle:

- **Stages of the information lifecycle** inc. creation, publication/use, retention/removal/deletion.
- **Concepts of the design process lifecycle,** inc. use of architectural frameworks; agile development; information sharing, service continuity.
- **Technical audit and review processes,** inc. vulnerability assessments and penetration tests; monitoring system and network access
- **Risks associated with systems development and support,** inc. open source/proprietary solutions; commercial off the shelf products; need for system separation and change control; preventing covert channels; handling patches; use of 'Escrow'.

Procedural/People Security Controls:

- **People risks,** inc. culture setting; need for awareness/ vetting/ contracts/codes of conduct/acceptable use policies/segregation of duties; obligations on interested parties.
- **Access controls to manage risks,** inc. authentication and authorisation; approaches to and administration of access control; access points; information classification.
- **Importance of appropriate training,** inc. need to tailor, different approaches; information sources, developing positive behaviour; continual professional development.

Technical Security Controls:

- **Protection against malicious software,** inc. types (e.g. trojans, botnets, viruses, worms, active content, ransomware); infection routes (e.g. phishing, click-bait); control methods; security by design and default and configuration management.
- **Underlying networks and communications systems,** inc. network entry points; network partitioning; role of cryptography; controlling 3rd party access; network and acceptable use policy; intrusion monitoring and detection; vulnerability assessment and penetration testing, secure network management.
- **Information security issues relating to value-added services,** inc. securing real time services; securing data exchange methods; protecting web servers; mobile computing, homeworking and BYOD; 3rd party information exchange.
- **Information security issues relating to the Cloud,** inc. legal implications; selecting Cloud computing providers; traditional computing risks vs. Cloud computing risks; commercial risks.
- **Security in information systems and how they apply to the IT infrastructure,** inc. security information and event monitoring (SIEM); separating systems; conforming with policies etc; modelling threats and attacks; recovery capabilities; intrusion monitoring, installation baseline control; protecting and promoting security development.

Physical and Environmental Security Controls

- **Need for multi-layered defences to protect information from environmental and physical risks ,** inc. access controls; protecting IT equipment, powers supplies, cabling etc; processes to handle business continuity incidents and events; clear desk and screen; moving and disposing of information assets; securing loading and delivery areas.

Disaster Recovery (DR) and Business Continuity (BC)

- **Differences between DR and BC and key elements,** inc. business impact analysis and risk assessment; resilience of systems; developing and testing plans; need for documentation and linking/involving internal and external resources; relationship with security incident management; compliance with standards such as ISO 22301.

Other Technical Aspects

- **Security investigations and forensics,** inc. common tools, processes and techniques, legal and regulatory guidelines, linking with law enforcement and specialist security advice; issues when buying in 3rd party forensic support.
- **Role of cryptography,** inc. theory, techniques and algorithm types; policies for cryptographic use, common key management approaches and requirements for cryptographic controls; common encryption models and common public key infrastructures and trust models; practical applications; use by individuals of encryption facilities within applications.

Course Cost

Please contact URM on 0118 206 5410 or email address info@urmconsulting.com

Locations

The training takes place at dedicated, residential training centres

Certified Training

in association with National Cyber Security Centre

APMG International

Chartered Institute of Information Security

bcs The Chartered Institute for IT

To register

For all enquiries, including dates, please contact 0118 206 5410 or info@urmconsulting.com