BCS Foundation Certificate in Information Security Management Principles Syllabus

Version 8.2
March 2017

This qualification is not regulated by the following United Kingdom Regulators - Ofqual, Qualification in Wales, CCEA or SQA

BCS Foundation Certificate in Information Security Management Principles

Change History

Any changes made to the syllabus shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

Version Number	Changes Made
V8.2 March 2017	Standardised new template format adopted, with revised ToC. Change of name to "Foundation Certificate" K levels added
V8.1 December 2016	Strapline regarding regulated statement has been added
V8.0 April 2016	1.1 Addition of cyber security, information assurance and information governance 2.1 Addition of threat intelligence, big data, the Internet of things and the vulnerabilities in social media and networks 2.2 Change of terminology to include strategic, tactical and operational options for dealing with risks 3.3 Addition of where to find standards 5.5 Addition of separation of systems Updates to relationship between syllabus and ISO/IEC 2700x:2013 standards
V 7.6 March 2015	Updated language requirements for extra time and use of dictionaries. Standardised the trainer criteria
V 7.5 October 2013	Book reference update. Trainer criteria updated. Updates to syllabus covering International Standards and Cyber Security.
V 7.4 October 2012	Minor text update to Section 3.1.5
V 7.3 September 2012	Trainer Qualification Criteria updated to remove 80% pass mark. Title page updated to add effective from date. Reference to ISEB removed where appropriate and replaced with BCS. Added a section to cover excerpts from BCS books
V 7.2 June 2011	5.1 Bullet 3 Changed protocol to project. 5.5 Bullet 6 Installation baselines is a new bullet 6.2 Bullet 4 Separation of development is a new bullet 6.2 Bullet 9 Handling of security patches is a new bullet
V 7.1 May 2011	Corrected a minor formatting error in Section 4.0
V 7.0 March 2011	Added Rationale / Background, Aims and Objectives, Target Group, Pre-Requisites, Direct Entry Route, Trainer Criteria, Specific Learning Objectives, Classroom Sizes, Notice to Accredited Training Organisations, Question Weighting, Syllabus References and Reading List, Skills and Knowledge Levels. Timings have been re-allocated and the syllabus re-ordered from 4 sections into 9 sections. Additional subject areas covered are: Technical Security Control, Cloud Computing, Software Development and Lifecycle. Removed Experience Route under Eligibility for the Examination.
V 5.5 November 2009	Reformatted with new branding. Added in Examination Format. No changes to the syllabus content.

Introduction

This certificate covers the range of concepts, approaches and techniques that are applicable to BCS Foundation Certificate in Information Security Management Principles. Candidates are required to demonstrate their knowledge and understanding of these aspects of BCS Foundation Certificate in Information Security Management Principles.

The certificate is relevant to anyone requiring an understanding of BCS Foundation Certificate in Information Security Management Principles including those who have information security responsibilities as part of their day to day role, or who are thinking of moving into an information security or related function.

It also provides the opportunity for those already within these roles to enhance or refresh their knowledge and in the process gain a qualification, recognised by industry, which demonstrates the level of knowledge gained.

Objectives

Candidates should be able to demonstrate knowledge and understanding of BCS Foundation Certificate in Information Security Management Principles and techniques. Key areas are:

- Knowledge of the concepts relating to information security management (confidentiality, integrity, availability, vulnerability, threats, risks, countermeasures)
- 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 has to operate
- Knowledge of the categorisation, operation and effectiveness of controls of different types and characteristics

It is recommended that candidates read the BCS book, ‘Information Security Management Principles’, which is the approved reference book for this qualification before taking this exam.

Target Audience

The certificate is relevant to anyone requiring an understanding of BCS Foundation Certificate in Information Security Management Principles 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. It is very much a firm foundation on which other qualifications can be built or which provides a thorough general understanding to enable business to ensure their information is protected appropriately.

Course Format and Duration

Candidates can study for this certificate in two ways: by attending an accredited training course provided by Accredited Training Organisation or by self-study. An accredited training course will require a minimum of 40 of study and practical work run over a minimum of five days.

The course can be delivered a number of different ways from traditional class-room based training to online e-learning.

Eligibility for the Examination

There are no specific pre-requisites for entry to the examination; however candidates should possess the appropriate level of knowledge to fulfil the objective shown above:

- A knowledge of IT would be advantageous but not essential
- An understanding of the general principles of information technology security would be useful
- Awareness of the issues involved with security control activity would be advantageous.

It is strongly recommended that you attend an accredited training course, however this is not mandatory. Candidates that have not attended an accredited training course should have some experience in the area of security with an understanding of the general principles of information technology security and an awareness of the issues involved with security control activity.

Format of the Examination

- Two hour ‘closed book’
- 100 multiple choice questions
- Pass mark is 65/100 (65%)
- Distinction mark is a minimum of 80/100

Additional time

For candidates requiring reasonable adjustments

Please refer to the reasonable adjustments policy for detailed information on how and when to apply.

For candidates whose language is not the language of the examination

If the examination is taken in a language that is not the candidate's native/official language, candidates are entitled to:

- 25% extra time
- Use their own **paper** language dictionary (whose purpose is translation between the examination language and another national language) during the examination Electronic versions of dictionaries will **not** be allowed into the examination room

Excerpts from BCS Books

Accredited Training Organisations may include excerpts from BCS books in the course materials. If you wish to use excerpts from the books you will need a license from BCS to do this. If you are interested in taking out a licence to use BCS published material you should contact the Head of Publishing at BCS outlining the material you wish to copy and the use to which it will be put.

Guidelines for Accredited Training Organisations

Each major subject heading in this syllabus is assigned an allocated time. The purpose of this is two-fold: first, to give both guidance on the relative proportion of time to be allocated to each section of an accredited course and an approximate minimum time for the teaching of each section; second, to guide the proportion of questions in the exam. Accredited Training Organisations may spend more time than is indicated and candidates may spend more time again in reading and research. Courses do not have to follow the same order as the syllabus. Courses may be run as a single module or broken down into two or three smaller modules.

This syllabus is structured into sections relating to major subject headings and numbered with a single digit section number. Each section is allocated a minimum contact time for presentation.

Syllabus

For each top-level area of the syllabus a percentage and K level is identified. The percentage is the exam coverage of that area, and the K level identifies the maximum level of knowledge that may be examined for that area.

1. Information Security Management Principles (10%, K2)

In this section, candidates will learn the basic concepts of information security together with the main terms in common usage.

Candidates will gain an understanding of why information security is becoming increasingly important not just in the IT community but also in the business community at large.

1.1 Concepts and Definitions

Note: This covers the definitions, meanings and use of concepts and terms across information security management. It includes the concepts and terms:

1.1.1 Information security (confidentiality, integrity, availability and non-repudiation)
1.1.2 Cyber security
1.1.3 Asset and asset types (information, physical, software)
1.1.4 Asset value and asset valuation
1.1.5 Threat, vulnerability, impact and risk
1.1.6 Information security policy concepts
1.1.7 The types, uses and purposes of controls
1.1.8 Identity, authentication, authorisation
1.1.9 Accountability, audit and compliance
1.1.10 Information security professionalism and ethics
1.1.11 The Information Security Management System (ISMS) concept
1.1.12 Information Assurance and Information Governance

1.2 The need for, and the benefits of information security

Note: This covers the way in which information security management relates to its environment. It includes:

1.2.1 Importance of information security as part of the general issue of protection of business assets and of the creation of new business models e.g. cloud, mergers, acquisitions and outsourcing
1.2.2 Different business models and their impact on security (e.g. online business vs. traditional manufacturing vs. financial services vs. retail; commercial vs. governmental)
1.2.3 Effect of rapidly changing information and business environment on information security
1.2.4 Balancing the cost/impact of security against the reduction in risk achieved
1.2.5 Information Security as part of overall company security policy
1.2.6 The need for a security policy and supporting standards, guidelines and procedures

1.2.7 The relationship with corporate governance and other areas of risk management

1.2.8 Security as an enabler; delivering value rather than cost

2. Information Risk (10%, K2)

In this section, candidates will gain an appreciation of risk assessment and management as it applies to information security. Candidates will learn how:

- Threats and vulnerabilities lead to risks
- Threats and vulnerabilities apply specifically to IT systems
- The business must assess the risks in terms of the impact suffered by the organisation should the risk materialise
- To determine the most appropriate response to a risk and the activities required to achieve the effective management of risks over time.

2.1 Threats to and vulnerabilities of information systems (5%)

Note: This covers the threats to, and vulnerabilities of information systems, and their contribution to risk. It includes:

2.1.1 Threat intelligence and sharing, the speed of change of threats and the need for a timely response

2.1.2 Threat categorisation (accidental vs. deliberate, internal vs. external, etc.)

2.1.3 Types of accidental threats (e.g. hazards, human error, malfunctions, fire, flood, etc.)

2.1.4 Types of deliberate threats (e.g. hacking, malicious software, sabotage, cyber terrorism, hi-tech crime, etc.)

2.1.5 Big Data, the Internet of Things and the Dark Web

2.1.6 Sources of accidental threat (e.g. internal employee, trusted partner, poor software design, weak procedures and processes, managed services, newsgroups, etc.)

2.1.7 Sources of deliberate threat (internal employee, trusted partner, random attacker, targeted attack, managed and outsourced services, web sites, etc.)

2.1.8 Vulnerability categorisation (e.g. weaknesses in software, hardware, buildings/facilities, people, procedures)

2.1.9 Vulnerabilities of specific information system types (e.g. PCs, laptops, hand held devices, Bring Your Own Devices (BYOD), servers, network devices, wireless systems, web servers, email systems, etc.)

2.1.10 The contribution of threats, vulnerabilities and asset value to overall risk

2.1.11 Impact assessment of realised threats (e.g. loss of confidentiality, integrity, and availability, leading to financial loss, brand damage, loss of confidence, etc.)

2.2 Risk Management (5%)

Note: This covers the processes for understanding and managing risk relating to information systems. It includes:

2.2.1 Risk management process (establish the context, assessment, including identification, analysis and evaluation; treatment, communication and consultation; and monitoring and review

2.2.2 Strategic options for dealing with risks (e.g. avoid/eliminate/terminate/reduce/ modify/transfer/accept/tolerate)

2.2.3 Tactical ways in which controls may be used – preventive, directive, detective and corrective

2.2.4 Operational types of controls – physical, procedural (people) and technical

2.2.5 The purpose of and approaches to impact assessment including qualitative quantitative, software tools and questionnaires

2.2.6 Identifying and accounting for the value of information assets

2.2.7 Principles of information classification strategies

2.2.8 The need to assess the risks to the business in business terms

2.2.9 Balancing the cost of information security against the cost of potential losses

2.2.10 The role of management in accepting risk

2.2.11 Contribution to corporate risk registers

3. Information Security Framework (20%, K3)

In this section, candidates will gain an understanding how risk management should be implemented in an organisation.

3.1 Organisation and Responsibilities (10%)

3.1.1 The organisation’s management of security

- Information security roles in an enterprise
- Placement in the organisation structure
- Board/Director responsibilities
- Responsibilities across the organisation
- Need to take account of statutory (e.g. data protection, health & safety), regulatory (e.g. financial services regulations) and advisory (e.g. accounting practices, corporate governance guidelines) requirements
- Provision of specialist information security advice and expertise
- Creating a culture of good information security practice

3.1.2 Organisational policy, standards and procedures

- Developing, writing and getting commitment to security policies
- Developing standards, guidelines, operating procedures, etc. internally and with third parties (outsourcing), managed service providers, etc.
- Balance between physical, procedural and technical security controls
- End user codes of practice
- Consequences of policy violation

3.1.3 Information Security Governance

- Review, evaluation and revision of security policy
- Security audits and reviews
- Checks for compliance with security policy
- Reporting on compliance status with reference to legal and regulatory requirements, e.g. Sarbanes Oxley

- Compliance of contractors, third parties and sub-contractors

3.1.4 Information Security implementation

- Planning – ensuring effective programme implementation
- How to present information security programmes as a positive benefit (e.g. business case, ROI case, competitive advantage, getting management buy-in)
- Security architecture and strategy
- Need to link with business planning and risk management and audit processes

3.1.5 Security Information management

Note: This covers incidents that affect the confidentiality, integrity or availability of information either directly or indirectly. This includes:

- Security incident reporting, recording, management
- Incident response teams/procedures
- Need for links to corporate incident management systems
- Processes for involving law enforcement or responding to requests from them

3.2 Legal Framework (5%)

Note: This section addresses general principles of law, legal jurisdiction and associated topics as they affect information security management. These will cover a broad spectrum from the security implications on compliance with legal requirements affecting business (e.g. international electronic commerce) to laws that directly affect the way information can be monitored and copied. Note that specific laws and legal issues relating to the country(s) within which a training provider operates may be mentioned as examples and included in course material, but the examination will only test the principles. Topics include:

3.2.1 Protection of personal data, restrictions on monitoring, surveillance, communications interception and trans-border data flows

3.2.2 Employment issues and employee rights (e.g. relating to monitoring, surveillance and communications interception rights and employment law)

3.2.3 Common concepts of computer misuse

3.2.4 Requirements for records retention

3.2.5 Intellectual property rights, e.g. copyright, including its application to software, databases and documentation

3.2.6 Contractual safeguards including common security requirements in outsourcing contracts, third party connections, information exchange, etc.

3.2.7 Collection of admissible evidence

3.2.8 Securing digital signatures (e.g. legal acceptance issues)

3.2.9 Restrictions on purchase, use and movement of cryptography technology

3.3 Security Standards and Procedures (5%)

Note: There are a number of common, established standards and procedures that directly affect information security management. Awareness of these to include:

3.3.1 Where to find national and international information security standards

3.3.2 ISO/IEC 27000 series, ISO/IEC 20000 (ITIL®), Common Criteria and other relevant international standards

3.3.3 International industry sector standards

3.3.4 Certification of information security management systems to appropriate standards – e.g. ISO/IEC 27001:2013

3.3.5 Product certification to recognised standards – e.g. ISO/IEC 15408 (the Common Criteria)
3.3.6 Key technical standards – e.g. IETF RFCs, FIPS, ETSI

4. Procedural/People Security Controls (15%, K3)

In this section, candidates will learn about the risks to information security involving people. Candidates will gain:

- An understanding of the controls that may be used to manage those risks
- An appreciation of the importance of appropriate training for all those involved with information

4.1 People (5%)

4.1.1 Organisational culture of security
4.1.2 Employee, contractor and business partner awareness of the need for security
4.1.3 Role of contracts of employment
4.1.4 Need for and topics within service contracts and security undertakings
4.1.5 Rights, responsibilities, authorities and duties of individuals - codes of conduct
4.1.6 Typical topics in acceptable use policies
4.1.7 Role of segregation of duties/avoiding dependence on key individuals
4.1.8 Typical obligations on interested parties (e.g. contractors, managed service providers, outsourced services, etc.)

4.2 User Access Controls (5%)

4.2.1 Authentication and authorisation mechanisms (e.g. passwords, tokens, biometrics, etc.) and their attributes (e.g. strength, acceptability, reliability)
4.2.2 Approaches to use of controls on access to information and supporting resources taking cognisance of data ownership rights (e.g. read/write/delete, control), privacy, operational access, etc.
4.2.3 Approaches to administering and reviewing access controls including role-based access, management of privileged users, management of users (joining, leaving, moving, etc.), emergency access
4.2.4 Access points – remote, local, web-based, email, etc. - and appropriate identification and authentication mechanisms
4.2.5 Information classification and protection processes, techniques and approaches

4.3 Training and Awareness (5%)

4.3.1 Purpose and role of training – need to tailor to specific needs of different interested parties (e.g. users vs. IT staff vs. business manager vs. customers)
4.3.2 Approaches to training and promoting awareness – e.g. videos, books, reports, computer based training and formal training courses

4.3.3 Sources of information, including internal and external conferences, seminars, newsgroups, trade bodies, government agencies, etc.
4.3.4 Developing positive security behaviour

5. Technical Security Controls (25%, K3)

In this section, candidates will learn about the technical controls that can be used to help ensure effective information security. Candidates will:

- Learn about the threats from malware
- Gain an understanding of the impact of those threats on networks and other communications systems
- Learn about the different approaches to information security required when dealing with out-sourced or other external facilities providers
- Learn about the importance of effective information security in all networked environments where there is information storage, processing or access being provided

5.1 Protection from Malicious Software (5%)

5.1.1 Types of malicious software – Trojans, botnets, viruses, worms, active content (e.g. Java, Active-X, XSS), etc.
5.1.2 Different ways systems can get infected
5.1.3 Methods of control – common approaches, need for regular updates, Open Web Application Security Project, etc.

5.2 Networks and Communications (5%)

Note: This subsection focuses on information security principles associated with the underlying networks and communications systems. This includes:
5.2.1 Entry points in networks and associated authentication techniques
5.2.2 Partitioning of networks to reduce risk – role of firewalls, routers, proxy servers and network boundary separation architectures
5.2.3 The role of cryptography in network security – common protocols and techniques (HTTPS, PKI, SSL/TLS, VPN, IPSec, etc.)
5.2.4 Controlling third party access (types of and reasons for) and external connections
5.2.5 Network and acceptable usage policy
5.2.6 Intrusion monitoring and detection methods and application
5.2.7 Vulnerability analysis and penetration testing of networks and connections
5.2.8 Secure network management (including configuration control and the periodic mapping and management of firewalls, routers, remote access points, wireless devices, etc.)

5.3 External Services (5%)

Note: This subsection focuses on the information security issues relating to value-added services that use the underlying networks and communications systems. This includes:

5.3.1 Securing real-time services (instant messaging, video conferencing, voice over IP, etc.)
5.3.2 Securing data exchange mechanisms e.g. e-commerce, email, internet downloads, file transfers, etc.
5.3.3 Protection of web servers and e-commerce applications
5.3.4 Mobile computing, home working and BYOD
5.3.5 Security of information being exchanged with other organisations
The management of information security within managed service and outsourced operations including during the circumstances of subsequent in-sourcing and changes of supplier

5.4 Cloud Computing (5%)

Note: This subsection focuses on the information security issues relating to organisations that utilise cloud computing facilities. Cloud computing is location independent computing providing off-site resources e.g. services, applications and storage facilities. This includes:

5.4.1 Legal implications for cloud computing notably for personal data, IPR and related issues
5.4.2 The particular information security considerations when selecting a cloud computing supplier
5.4.3 Comparing the risks of maintaining a ‘classical’ organisation and architecture with the risks in a cloud computing environment
5.4.4 The importance of distinguishing between commercial risk (of a supplier) and the other consequences of risk to the purchaser

5.5 IT Infrastructure (5%)

Note: This covers all aspects of security in information systems, including operating systems, database and file management systems, network systems and applications systems. This includes:

5.5.1 Security Information and Event Monitoring (SIEM)
5.5.2 Separation of systems to reduce risk
5.5.3 Conformance with security policy, standards and guidelines
5.5.4 Access control lists and roles, including control of privileged access
5.5.5 Correctness of input and on-going correctness of all stored data including parameters for all generalised software
5.5.6 Recovery capability, including back-up and audit trails
5.5.7 Intrusion monitoring, detection methods and application
5.5.8 Installation baseline controls to secure systems and applications - dangers of default settings
5.5.9 Configuration management and operational change control
5.5.10 The need to protect system documentation and promote security documentation within the organisation, within partner organisations and within

managed service and outsourced operations

6. Software Development and Lifecycle (5%, K3)

In this section, candidates will learn about the risk to security brought about by the development and full lifecycle of software. Candidates will:

- Gain an understanding of the importance of appropriate audit and review processes, of effective change control and of configuration management
- Learn about the differences for security between open source and proprietary solutions, commercial off the shelf and bespoke systems, and certified and non-certified systems
- Learn about some of the techniques involved in reducing the security risks in the development of code

6.1 Testing, Audit and Review

6.1.1 Methods and strategies for security testing of business systems, including vulnerability analysis and penetration testing
6.1.2 Need for correct reporting of testing and reviews
6.1.3 Verifying linkage between computer and clerical processes
6.1.4 Techniques for monitoring system and network access and usage including the role of audit trails, logs and intrusion detection systems, and techniques for the recovery of useful data from them

6.2 Systems Development and Support

6.2.1 Security requirement specification
6.2.2 Security involvement in system and product assessment – including open source vs proprietary solutions
6.2.3 Security issues associated with commercial off-the-shelf systems/applications/ products
6.2.4 Importance of links with the whole business process – including clerical procedures
6.2.5 Separation of development and support from operational systems
6.2.6 Security of acceptance processes and security aspects in process for authorising business systems for use
6.2.7 Role of accreditation of new or modified systems as meeting their security policy
6.2.8 Change control for systems under development to maintain software integrity
6.2.9 Security issues relating to outsourcing software development
6.2.10 Preventing covert channels, Trojan code, rogue code, etc. – code verification techniques
6.2.11 Handling of security patches
6.2.12 Use of certified products/systems
6.2.13 Use of “Escrow” to reduce risk of loss of source code

7. Physical and Environmental Security Controls (5%, K2)

In this section, candidates will gain an understanding of the physical aspects of security available in multi-layered defences.

Candidates will learn about the environmental risks to information in terms of the need, for example, for appropriate power supplies, protection from natural risks (fire, flood etc.) and in the everyday operations of an organisation.

Note: There is a need for information security managers to have a good appreciation of associated physical security issues, so they can make sure there is a seamless information security management system across the whole organisation. This includes:

- General controls on access to and protection of physical sites, offices, secure areas, cabinets and rooms
- Protection of IT equipment – servers, routers, switches, printers, etc.
- Protection of non-IT equipment, power supplies, cabling, etc.
- Need for processes to handle intruder alerts, deliberate or accidental physical events, etc.
- Clear screen and desk policy
- Moving property on and off-site
- Procedures for secure disposal of documents, equipment, storage devices, etc.
- Procedures for the disposal of equipment with digital-data retention facilities e.g. faxes, multi-function devices, photocopiers, network printers, etc.
- Security requirements in delivery and loading areas

8. Disaster Recovery and Business Continuity Management (5%, K2)

In this section, candidates will learn about the differences between and the need for business continuity and disaster recovery.

- Relationship with risk assessment and impact analysis
- Approaches to writing and implementing plans
- Need for documentation, maintenance and testing of plans
- Need for links to managed service provision and outsourcing
- Need for secure off-site storage of vital material
- Need to involve personnel, suppliers, IT systems providers, etc.
- Relationship with security incident management
- Compliance with standards - ISO 22301 series or other relevant international standards

9. Other Technical Aspects (5%, K2)

In this section, candidates will gain an understanding of the important aspects of incident investigation and how the forensic evidence may be preserved. Candidates will learn about the basic concepts and uses of cryptography.

9.1 Investigations and Forensics

Note: Information security managers need a good appreciation of the principles and common practices, including any legal constraints and obligations, so they can contribute appropriately to investigations.

9.1.1 Common processes, tools and techniques for conducting investigations
9.1.2 Legal and regulatory guidelines for investigations and evidence preservation
9.1.3 Need for relations with law enforcement, including specialist computer crime units
9.1.4 Issues when buying-in forensics and investigative support from third parties

9.2 Role of Cryptography

Note: Information security managers need an appreciation of the role of cryptography in protecting systems and assets, including awareness of the relevant standards and practices

9.2.1 Basic cryptographic theory, techniques and algorithm types, their use in confidentiality and integrity mechanisms and common cryptographic standards
9.2.2 Policies for cryptographic use, common key management approaches and requirements for cryptographic controls
9.2.3 Link, file, end-to-end, and other common encryption models and common Public Key Infrastructures and trust models e.g. two-way trust
9.2.4 Common practical applications of cryptography – e.g. for digital signatures, authentication and confidentiality

Levels of Knowledge / SFIA Levels

This course will provide candidates with the levels of difficulty / knowledge skill highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated. The levels of knowledge and SFIA levels are explained in on the website www.bcs.org/levels. The levels of knowledge above will enable candidates to develop the following levels of skill to be able to operate at the following levels of responsibility (as defined within the SFIA framework) within their workplace:

Level	Levels of Knowledge	Levels of Skill and Responsibility (SFIA)
K7		Set strategy, inspire and mobilise
K6	Evaluate	Initiate and influence
K5	Synthesise	Ensure and advise
K4	Analyse	Enable
K3	Apply	Apply
K2	Understand	Assist
K1	Remember	Follow

Question Weighting

Syllabus Area	Syllabus Code (New)	Syllabus Code (Old)	Time weightings (%)	Target number of questions
1. Information Security Management Principles				
Concepts and definitions	1.1	1.1	5	3
The need for and benefits of Information Security	1.2	1.2	5	4
2. Information Risk				
Threats to and vulnerabilities of information systems	2.1	2.1	5	8
Risk Management	2.2	2.2	5	7
3. Information Security Framework				
Organisation and responsibilities	3.1	3.1		
The organisation's management of security	3.1.1	3.1.1	10	3
Organisational policy, standards and procedures	3.1.2	3.1.2		3
Information security governance	3.1.3	3.1.3		3
Information security implementation	3.1.4	3.1.5		3
Security incident management	3.1.5	3.1.4		3
Legal framework	3.2	3.1.6	5	3
Security standards and procedures	3.3	3.1.7	5	3
4. Procedural/people security controls				

People	4.1	4.2	5	4
User access controls	4.2	4.3	5	3
Training	4.3	4.10	5	4
5. Technical security controls				
Protection from malicious software	5.1	4.1	5	4
Networks and communications	5.2	4.4	5	7
External services	5.3	4.5	5	3
Cloud computing	5.4	New	5	4
IT infrastructure	5.5	4.6	5	7
6. Software development				
Testing, audit & review	6.1	4.7	5	3
Systems development & support	6.2	4.8		4
7. Physical and environmental controls	7	4.11	5	3
8. Disaster recovery and business continuity management	8	4.12	5	6
9. Other technical aspects				
Investigations and forensics	9.1	4.13	5	2
Role of cryptography	9.2	4.9		3
	Total		100	100

Relationship between this syllabus and ISO2700x:2013 Standards

There is not a simple direct relationship between this syllabus and either ISO/IEC 27001:2013 or ISO/IEC27002:2013. These tables show the main syllabus reference for each section in both standards.

ISO/IEC 27001	This Syllabus	Topic
4		**Context of the organisation**
4.1	3.1.1	Understanding the organisation
4.2	3.1.1	Understanding the needs and expectations of interested parties
4.3	3.1.2	Determining the scope of the information security management system
4.4	3.1.2	Information security management system
5		**Leadership**
5.1	3.1.1	Leadership and commitment
5.2	3.1.2	Policy
5.3	3.1.1	Organisational roles, responsibilities and authorities
6		**Planning**
6.1	3.1.4	Actions to address risks and opportunities
6.2	3.1.4	Information security objectives and planning to achieve them
7		**Support**
7.3	4.3	Awareness
8		**Operation**
8.2	2.2	Information security risk assessment
8.3	4,5,6,7,8,9	Information security risk treatment

ISO/IEC 27002	This Syllabus	Topic
7		**Human resource security**
7.1	4.1	Prior to employment
7.2	4.1	During employment
7.3	4.1	Termination and change of employment
8		**Asset Management**
8.2	2.2	Information Classification
9		**Access Control**
9.1	4.2	Business requirements of access control
9.2	4.2	User access management
9.3	4.3	User responsibilities
9.4	4.2	System and application access control
10		**Cryptography**
10.1	5.2	Cryptographic models
11		**Physical and environmental security**
11.1	7	Secure areas
11.2	7	Equipment
12		**Operations security**
12.2	5.1	Protection from malware
12.3	5.5	Backup
12.4	5.5	Logging and monitoring
12.5	5.5	Control of operational software
12.6	5.2	Technical vulnerability management
12.7	6.1	Information systems audit considerations
13		**Communications security**
13.1	5.2	Network security management
13.2	5.2	Information transfer
14		**System acquisition, development and maintenance**
14.1	6.2	Security requirements of information systems
14.2	6.2	Security in development and support processes
14.3	6.1	Test data
15		**Supplier Relationships**
15.1	5.3	Information security in supplier relationships
15.2	5.3, 5.4	Supplier service delivery management
16		**Information security incident management**
16.1	3.1.5	Management of information security incidents and improvements
17		**Information Security aspects of business continuity management**
17.1	8	Information security continuity
17.2	8	Redundancies
18		**Compliance**
18.1	3.2	Compliance with legal and contractual requirements

Format of Examination

Type	100 Questions Multiple Choice
Duration	2 Hours. An additional 30 minutes will be allowed for candidates sitting the examination in a language that is not their native /mother tongue.
Pre-requisites	Accredited training is strongly recommended but is not a pre-requisite
Supervised	Yes
Closed Book	Yes
Pass Mark	65/100 (65%)
Distinction Mark	80/100 (80%)
Calculators	Calculators cannot be used during this examination.
Learning Hours	40 Hours
Delivery	Paper based examination via a BCS Accredited Training Organisation. Also available online

Trainer Criteria

Criteria	▪ Hold the BCS Information Security Management Principles Certificate ▪ Have an in-depth knowledge of the Information Security standards ▪ Have a good understanding of risk management tools and techniques ▪ Have 3 years' practical experience in information security/risk management ▪ Have 10 days' training experience or have a train the trainer qualification

Classroom Size

Trainer to candidate ratio	1:16

Recommended Reading List

Title	Information Security Management Principles 2nd edition
Authors	David Alexander, Amanda Finch, David Sutton, Andy Taylor
Publisher:	BCS, Learning and Development Limited
Publication:	June 2013 – 2nd edition
ISBN	9781780171753

Syllabus References

- ISO 27001:2013 A specification for an information security management system
- COBIT Framework Framework for IT Governance and Control
- ITIL - IT Infrastructure for Service Management
- The Institute for Information Security Professionals (IntstISP)
- Get Safe On-Line UK Government site for providing advice to the general population about secure computing
- CPNI - Centre for the Protection of National Infrastructure UK Government site for the protection of the critical national infrastructure
- BCS Information Security Specialist Group

Common Standards

- ISO 31000:2009– Risk Management Principles and Guidelines
- ISO31010:2010 – Risk Management – Risk Assessment Techniques
- COSO 2004 – Enterprise Risk Management Integrated Framework (due to be updated in 2015)
- OCEG Red Book 2009 A Governance, Risk and Compliance Capability Model
- ISO Guide 73:2009 Definitions of generic terms related to Risk Management
- ISO 27005:2011 Guidelines for information security risk management
- BS 31100:2011

There are a significant number of other books, web sites and professional organisations which can provide relevant and extended information to support this examination course.

Note that a standard will take precedence over a book. Where common practice differs from standard, candidates will not be penalised for using a standard approach. Nevertheless, candidates should show an awareness of the differences from standard.