bcs
The
Chartered
Institute
for IT

Certificate in Information Security Management Principles Syllabus

Version 7.2

June 2011

Contents

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 the changes made. The purpose is to be able to identify quickly what changes have been made.

Version Number and Date of Change	Changes Made
V7.2 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
V7.1 May 2011	Corrected a minor formatting error in Section 4.0
V7.0 March 2011	Added Rationale / Background, Aims and Objectives, Target Group, Pre-Requisites, Direct Entry Route, Trainer Criteria, Specific Learning Objectives, Classroom Sizes, Notice to Training Providers, 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.
V5.5 November 2009	Reformatted with new branding. Added in Examination Format. No changes to the syllabus content.

Rationale / Background

The Certificate in Information Security Management Principles is designed to provide the foundation of knowledge necessary for individuals 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.

Aims and Objectives

The qualification will prove that the holder has a good knowledge and basic understanding of the wide range of subject areas that make up information security management. The syllabus is, therefore, as far as possible, technology neutral. The qualification tests knowledge of principles, not knowledge of specific technologies or products. Note that course material may use specific technical examples to illustrate particular principles, but it is the principles that should be understood from any such use of examples.

Target Group

The examination is intended for 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 more technical qualifications can be built or which provides a thorough general understanding to enable business users of IT to ensure their information is protected appropriately.

Prerequisite Entry Criteria for the Course

- 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
- There is no pre-course study set by ISEB although individual Training Providers may choose to set some

Eligibility for the Examination

Training Route

It is strongly recommended that candidates attend an accredited training course.

Experienced Route (Not attending the course)

It is recommended that candidates 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.

In addition, it is recommended that candidates read the ISEB 'Information Security Management Principles' which is the approved reference book for this qualification before taking this exam.

Format of the Examination

Type	100 Question Multiple Choice Examination
Duration	2 Hour Examination
Supervised / Invigilated	Yes
Closed Book	Yes, no reading materials allowed into the examination room
Pass Mark	65%
Distinction Mark	80%
Delivery	Paper based examination via an Accredited Training Provider or via the direct entry sittings in the BCS London offices.

Specific Learning Objectives

On completion of training against this syllabus, candidates should be able to demonstrate:

- Knowledge of the concepts relating to information security management (confidentiality, integrity, availability, vulnerability, threats, risks, countermeasures, etc);
- 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.

Notice to Training Providers

Each major subject heading in the syllabus is assigned an allocated time. The purpose of this is 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. Training Providers may spend more time than is indicated and candidates may spend more time again in reading and research.

The total time specified in this syllabus is 40 hours of lecture and practical work.

The course may be delivered as a series of modules with gaps between them, as long as it meets all other constraints. Courses do not have to follow the same order as the syllabus.

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.

Syllabus

1. Information Security Management Principles – 10%

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

They 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 - 5%

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

- Information security (confidentiality, integrity, availability, non-repudiation)
- Asset and asset types (information, physical, software);
- Asset value and asset valuation
- Threat, vulnerability, impact, risk,
- Information security policy concepts
- The types, uses and purposes of controls
- Identity, authentication, authorisation
- Accountability, audit and compliance
- Information security professionalism and ethics
- The Information Security Management System (ISMS) concept

1.2 The Need for, and the Benefits of Information Security - 5%

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

- 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.
- Different business models and their impact on security (e.g. on-line business vs. traditional manufacturing vs. financial services vs. retail).
- Effect of rapidly changing information and business environment on information security.
- Balancing the cost/impact of security against the reduction in risk achieved.
- Information Security as part of overall company security policy.
- The need for a security policy and supporting standards, guidelines and procedures.
- The relationship with corporate governance and other areas of risk management.
- Security as an enabler; delivering value rather than cost.
- Role of information security in countering hi-tech crime – revitalised old crimes, new types of crime.

2. Information Risk – 10%

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

- They will learn how threats and vulnerabilities lead to risks.
- They will gain an understanding of how threats and vulnerabilities apply specifically to IT systems.
- They will understand how the business must assess the risks in terms of the impact suffered by the organisation should the risk materialise.
- They will learn how 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:

- Threat categorisation (accidental vs. deliberate, internal vs. external, etc.)
- Types of accidental threats (e.g. human error, malfunctions, fire, flood, etc.)
- Types of deliberate threats (e.g. hacking, malicious software, sabotage, cyber terrorism, hi-tech crime, etc.)
- Sources of accidental threat (e.g. internal employee, trusted partner, poor software design, weak procedures & processes, managed services, newsgroups, etc.)
- Sources of deliberate threat (internal employee, trusted partner, random attacker, targeted attack, managed and outsourced services, web sites, etc.)
- Vulnerability categorisation (e.g. weaknesses in software, hardware, buildings/facilities, people, procedures)
- Vulnerabilities of specific information system types (e.g. PCs, laptops, hand held devices, servers, network devices, wireless systems, web servers, e-mail systems, etc.)
- The contribution of threats, vulnerabilities and asset value to overall risk.
- Business impact 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:

- Risk management process (identification, analysis, mitigation and monitoring of risks)
- Options for dealing with risks (e.g. eliminate, reduce, transfer, accept; or avoid, accept, reduce, transfer; or terminate, tolerate, treat, transfer)
- Different ways in which controls may be used - preventative, directive, detective and corrective.
- Different types of controls - physical, procedural (people) and technical
- The purpose of risk assessment/analysis - strategic and tactical options
- Approaches to risk analysis/assessment - qualitative, quantitative, software tools, questionnaires.
- Identifying and accounting for the value of information assets
- Principles of information classification strategies
- The need to assess the risks to the business in business terms
- Balancing the cost of information security against the cost of potential losses
- The role of management in accepting risk
- Contribution to corporate risk registers

3. Information Security Framework – 20%

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

- They will learn the importance of the organisation's policies, standards and procedures.
- They will learn the importance of effective governance in managing information security.
- They will learn how to plan for and to deal with an information security incident.
- They will gain an understanding of the relevant legal framework with which an organisation must comply.
- They will learn about the national and international standards that are applicable to information security.

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 responsibility
- 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, 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

3.1.1 Security Incident Management

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

- Security incident reporting, recording and 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:

- Protection of personal data, restrictions on monitoring, surveillance, communications interception and trans-border data flows
- Employment issues and employee rights (e.g. relating to monitoring, surveillance and communications interception rights and employment law)
- Common concepts of computer misuse
- Requirements for records retention
- Intellectual property rights, e.g. copyright, including its application to software, databases, documentation
- Contractual safeguards including common security requirements in outsourcing contracts, third party connections, information exchange, etc.
- Collection of admissible evidence
- Securing digital signatures (e.g. legal acceptance issues)
- 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:

- ISO/IEC 27000 series, ISO/IEC20000 (ITIL®), Common Criteria and other relevant international standards
- International industry sector standards
- Certification of information security management systems to appropriate standards – e.g. ISO/IEC 27001:2005
- Product certification to recognised standards – e.g. ISO/IEC 15408 (the Common Criteria)
- Key technical standards – e.g. IETF RFCs, FIPS, ETSI

4. Procedural / People Security Controls – 15%

In this section candidates will learn about the risks to information security involving people.

- They will gain an understanding of the controls that may be used to manage those risks.
- They will gain an appreciation of the importance of appropriate training for all those involved with information.

4.1 People - 5%

- Organisational culture of security
- Employee, contractor and business partner awareness of the need for security
- Role of contracts of employment
- Need for and topics within service contracts and security undertakings
- Rights, responsibilities and duties of individuals - codes of conduct
- Typical topics in acceptable use policies
- Role of segregation of duties/avoiding dependence on key individuals
- Typical obligations on third party providers and staff (e.g. contractors, managed service providers, outsourced services, etc.)

4.2 User Access Controls – 5%

- Authentication and authorisation mechanisms (e.g. passwords, tokens, biometrics, etc.) and their attributes (e.g. strength, acceptability, reliability)
- 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.
- Approaches to administering access controls including role-based access, management of privileged users, management of users (joining, leaving, moving, etc.), emergency access, etc.
- Access points – remote, local, web-based, e-mail, etc. - and appropriate identification and authentication mechanisms
- Information classification and protection processes, techniques and approaches

4.3 Training and Awareness - 5%

- Purpose and role of training – need to tailor to specific needs of different audiences (e.g. users vs. IT staff vs. business managers vs. customers).
- Approaches to training and promoting awareness – e.g. videos, books, reports, CBT and formal training courses
- Sources of information, including internal and external conferences, seminars, newsgroups, trade bodies, government agencies, etc.
- Developing positive security behaviour

5. Technical Security Controls – 25%

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

- They will learn about the threats from malware.
- They will gain an understanding of the impact of those threats on networks and other communications systems.
- They will learn about the different approaches to information security required when dealing with out-sourced or other external facilities providers.
- They will 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%

- Types of malicious software – Trojans, botnets, viruses, worms, active content (e.g. Java, Active-X, XSS), etc.
- Different ways systems can get infected
- 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:

- Entry points in networks and associated authentication techniques
- Partitioning of networks to reduce risk – role of firewalls, routers, proxy servers and network boundary separation architectures
- The role of cryptography in network security – common protocols & techniques (HTTPS, PKI, SSL, VPN, IPSec, etc.)
- Controlling third party access (types of and reasons for) and external connections
- Network and acceptable usage policy
- Intrusion monitoring and detection methods and application
- Vulnerability analysis & penetration testing of networks and connections
- 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:

- Securing real-time services (instant messaging, video conferencing, voice over IP, etc.)
- Securing data exchange mechanisms e.g. e-commerce, e-mail, internet downloads, file transfers, etc.
- Protection of web servers and e-commerce applications
- Mobile computing and home working
- 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:

- Legal implications for cloud computing notably for personal data, IPR and related issues
- The particular information security considerations when selecting a cloud computing supplier
- Comparing the risks of maintaining a ‘classical’ organisation and architecture with the risks in a cloud computing environment
- 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:

- Separation of systems to reduce risk
- Conformance with security policy, standards and guidelines
- Access control lists and roles, including control of privileged access
- Correctness of input and on-going correctness of all stored data including parameters for all generalised software
- Recovery capability, including back-up and audit trails
- Intrusion monitoring and detection methods and application
- Installation baseline controls to secure systems and applications - dangers of default settings
- Configuration management and operational change control
- 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%

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

- They will gain an understanding of the importance of appropriate audit and review processes, of effective change control and of configuration management.
- They will 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
- They will learn about some of the techniques involved in reducing the security risks in the development of code.

6.1 Testing, Audit and Review

- Methods and strategies for security testing of business systems, including vulnerability analysis and penetration testing
- Need for correct reporting of testing and reviews
- Verifying linkage between computer and clerical processes
- 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

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

7. Physical and Environmental Security Controls – 5%

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

They 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, 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 & 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 device, photocopiers, network printers, etc.
- Security requirements in delivery and loading areas

8. Disaster Recovery and Business Continuity Management – 5%

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 - BS 25999series or other relevant international standards

9. Other Technical Aspects – 5%

In this section candidates will gain an understanding of the important aspects of incident investigation and how the forensic evidence may be preserved. They 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.

- Common processes, tools and techniques for conducting investigations
- Legal and regulatory guidelines for investigations and evidence preservation.
- Need for relations with law enforcement, including specialist computer crime units.
- 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.

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

Question Weighting

Section title	Syllabus code (New)	Syllabus code (Old)	Time weightings (%)	Avg. target number of questions per paper
1. Information Security Management Principles				
Concepts and definitions	1.1	1.1	5	3
The need for & benefits of Information Security	1.2	1.2	5	4
2. Information Risk				
Threats to & 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 & 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 & forensics	9.1	4.13	5	2
Role of cryptography	9.2	4.9		3
	Total		100	100

Relationship between this Syllabus and ISO/IEC27001:2005

There is not a simple direct relationship between this syllabus and ISO/IEC27001:2005. This table shows the main syllabus reference for each section in ISO/IEC27001:2005 standard.

ISO/IEC 27001	This Syllabus	Topic
4.1	2.1	Assessing security risks
4.2	2.2	Treating security risks
5.1.1	3.1.1	Information security policy document
5.1.2	3.1.2	Review of information security policy
6.1	3.1	Internal organisation
6.2	4.1	External parties
7.1	1.2	Responsibility for assets
7.2	2.2	Information classification
8	4.1	Human resources security
9	7	Physical and environmental security
10.1	5.5	Operational procedures and responsibilities
10.2	4.1	Third part service delivery management
10.3	6.2	System planning and acceptance
10.4	5.1	Protection against malicious and mobile code
10.5	5.5	Back-up
10.6	5.2	Network security management
10.7	7	Media handling
10.8	5.3	Exchange of information
10.9	5.3	Electronic commerce services
10.10	5.5	Monitoring
11.1	4.2	Business requirement for access control
11.2	4.2	User access management
11.3	4.2	User responsibilities
11.4	5.2	Network access control
11.5	4.2	Operating system access control
11.6	4.2	Application and information access control
11.7	5.3	Mobile computing and teleworking
12.1	6.2	Security requirements of information systems
12.2	6.2	Correct processing in applications
12.3	9.2	Cryptographic controls
12.4	5.5	Security of system files
12.5	6.2	Security in development and support processes
12.6	6.2	Technical vulnerability management
13.1	3.1.3	Reporting information security events and weaknesses
13.2	9.1	Management of information security incidents and improvements
14	8	Business continuity management
15.1	3.2	Compliance with legal requirements

Syllabus References and Reading Lists

- Information Security Management Principles: An ISEB Certificate
  David Alexander, Amanda French, David Sutton, Andy Taylor
  ISBN: 9781902505909 Paperback from BCS Bookshop

- ISO/IEC 27001:2005 and related standards includingBS25999. British Standards Institute www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/

- COBIT framework for IT governance and control - www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

- ITIL - IT Infrastructure Library for service management of IT – www.itil-officialsite.com/home/home.asp

- The Institute for Information Security Professionals (InstISP) - www.instisp.org/

    - UK Government web site providing advice for the general population about secure computing – www.getsafeonline.org

    - UK Government web site for the protection of the critical national infrastructure – www.cpni.gov.uk

- British Computer Society Information Security Specialist Group – www.bcs-issg.org.uk/index.html

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.

Additional Information

Levels of Skill and Responsibility (SFIA 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 1: Follow

Work under close supervision to perform routine activities in a structured environment. They will require assistance in resolving unexpected problems, but will be able to demonstrate an organised approach to work and learn new skills and applies newly acquired knowledge.

Level 2: Assist

Works under routine supervision and uses minor discretion in resolving problems or enquiries. Works without frequent reference to others and may have influence within their own domain. They are able to perform a range of varied work activities in a variety of structured environments and can identify and negotiate their own development opportunities. They can also monitor their own work within short time horizons and absorb technical information when it is presented systematically and apply it effectively.

Level 3: Apply

Works under general supervision and uses discretion in identifying and resolving complex problems and assignments. They usually require specific instructions with their work being reviewed at frequent milestones, but can determines when issues should be escalated to a higher level. Interacts with and influences department/project team members. In a predictable and structured environment they may supervise others. They can perform a broad range of work, sometimes complex and non-routine, in a variety of environments. They understand and use appropriate methods, tools and applications and can demonstrate an analytical and systematic approach to problem solving. They can take the initiative in identifying and negotiating appropriate development opportunities and demonstrate effective communication skills, sometimes planning, scheduling and monitoring their own work. They can absorb and apply technical information, works to required standards and understand and uses appropriate methods, tools and applications.

Level 4: Enable

Works under general direction within clear framework of accountability and can exercise substantial personal responsibility and autonomy. They can plan their own work to meet given objectives and processes and can influence their team and specialist peers internally. They can have some responsibility for the work of others and for the allocation of resources. They can make decisions which influence the success of projects and team objectives and perform a broad range of complex technical or professional work activities, in a variety of contexts. They are capable of selecting appropriately from applicable standards, methods, tools and applications and demonstrate an analytical and systematic approach to problem solving, communicating fluently orally and in writing, and can present complex technical information to both technical and non-technical audiences. They plan, schedule and monitor their work to meet time and quality targets and in accordance with relevant legislation and procedures, rapidly absorbing new technical information and applying it effectively. They have a good appreciation of the wider field of information systems, their use in relevant employment areas and how they relate to the business activities of the employer or client.

Level 5: Ensure and advise

Works under broad direction, being fully accountable for their own technical work and/or project/supervisory responsibilities, receiving assignments in the form of objectives. Their work is often self-initiated and they can establish their own milestones, team objectives, and candidates responsibilities. They have significant responsibility for the work of others and for the allocation of resources, making decisions which impact on the success of assigned projects i.e. results, deadlines and budget. They can also develop business relationships with customers, perform a challenging range and variety of complex technical or professional work activities and undertake work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. They can advise on the available standards, methods, tools and applications relevant to own specialism and can make correct choices from alternatives. They can also analyse, diagnose, design, plan, execute and evaluate work to time, cost and quality targets, communicating effectively, formally and informally, with colleagues, subordinates and customers. They can demonstrate leadership, mentor more junior colleagues and take the initiative in keeping their skills up to date. Takes customer requirements into account and demonstrates creativity and innovation in applying solutions for the benefit of the customer.

Level 6: Initiate and influence

Have a defined authority and responsibility for a significant area of work, including technical, financial and quality aspects. They can establish organisational objectives and candidates responsibilities, being accountable for actions and decisions taken by them self and their subordinates. They can influence policy formation within their own specialism to business objectives, influencing a significant part of their own organisation and customers/suppliers and the industry at senior management level. They make decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance, developing high-level relationships with customers, suppliers and industry leaders. They can perform highly complex work activities covering technical, financial and quality aspects. They contribute to the formulation of IT strategy, creatively applying a wide range of technical and/or management principles. They absorb complex technical information and communicate effectively at all levels to both technical and non-technical audiences, assesses and evaluates risk and understand the implications of new technologies. They demonstrate clear leadership and the ability to influence and persuade others, with a broad understanding of all aspects of IT and deep understanding of their own specialism(s). They take the initiative in keeping both their own and subordinates' skills up to date and to maintain an awareness of developments in the IT industry.

Level 7: Set strategy, inspire and mobilise

Have the authority and responsibility for all aspects of a significant area of work, including policy formation and application. They are fully accountable for actions taken and decisions made, by both them self and their subordinates. They make decisions critical to organisational success and influence developments within the IT industry at the highest levels, advancing the knowledge and/or exploitation of IT within one or more organisations. They develop long-term strategic relationships with customers and industry leaders, leading on the formulation and application of strategy. They apply the highest level of management and leadership skills, having a deep understanding of the IT industry and the implications of emerging technologies for the wider business environment. They have a full range of strategic management and leadership skills and can understand, explain and present complex technical ideas to both technical and non-technical audiences at all levels up to the highest in a persuasive and convincing manner. They have a broad and deep IT knowledge coupled with equivalent knowledge of the activities of those businesses and other organisations that use and exploit IT. Communicates the potential impact of emerging technologies on organisations and individuals and analyses the risks of using or not using such technologies. They also assess the impact of legislation, and actively promote compliance.

Levels of Knowledge (K Levels)

The following levels of knowledge shall be defined and applied for syllabus creation. Each topic in the syllabus shall be examined according to the learning objectives defined in the section devoted to that topic. Each learning objective has a level of knowledge (K level) associated with it and this K level by association defines the nature of any examination questions related to that topic.

Note that each K level subsumes lower levels. For example, a K4 level topic is one for which a candidate must be able to analyse a situation and extract relevant information. A question on a K4 topic could be at any level up to and including K4. As an example, a scenario requiring a candidate to analyse a scenario and select the best risk identification method would be at K4, but questions could also be asked about this topic at K3 and a question at K3 for this topic might require a candidate to apply one of the risk identification methods to a situation.

Level 1: Remember (K1)

The candidate should be able to recognise, remember and recall a term or concept but not necessarily be able to use or explain. Typical questions would use: define, duplicate, list, memorise, recall, repeat, reproduce, state.

Level 2: Understand (K2)

The candidate should be able to explain a topic or classify information or make comparisons. The candidate should be able to explain ideas or concepts. Typical questions would use: classify, describe, discuss, explain, identify, locate, recognise, report, select, translate, paraphrase.

Level 3: Apply (K3)

The candidate should be able apply a topic in a practical setting. The candidate should be able to use the information in a new way. Typical questions would use: choose, demonstrate, employ, illustrate, interpret, operate, schedule, sketch, solve, use, write.

Level 4: Analyse (K4)

The candidate should be able to distinguish/separate information related to a concept or technique into its constituent parts for better understanding, and can distinguish between facts and inferences. Typical questions would use: appraise, compare, contrast, criticise, differentiate, discriminate, distinguish, examiner, question, test.

Level 5: Synthesise (K5)

The candidate should be able to justify a decision and can identify and build patterns in facts and information related to a concept or technique, they can create new meaning or structure from parts of a concept. Typical questions would use: appraise, argue, defend, judge, select, support, value, evaluate.

Level 6: Evaluate (K6)

The candidate should be able to provide a new point of view and can judge the value of information and decide on its applicability in a given situation. Typical questions would use: assemble, contract, create, design, develop, formulate, write.

Learning objectives are given indicators from K1-K6. These are based on Bloom's taxonomy of knowledge in the cognitive domain (ref Taxonomy of Educational Objectives, Handbook 1 – The Cognitive Domain, Bloom et al., New York 1956), and can be broadly interpreted as follows: K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyse; K5 – Synthesise; K6 – Evaluate. Bloom's taxonomy is explained in greater detail in Section 5.1. All topics shall have learning objectives associated with them, each of which has an associated K level. The language used must, as far as possible, mirror the language used in defining Bloom's taxonomy to provide candidates with consistent pointers to the expected level of knowledge and a consistent way of expressing that level in words.

This course will provide candidates with the levels of knowledge highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated. The levels of knowledge, skill and responsibility are explained in the following text:

Level	Levels of knowledge	Levels of skill and responsibility
7		Set strategy, inspire and mobilise
6	Evaluate	Initiate and influence
5	Synthesise	Ensure and advise
4	Analyse	Enable
3	Apply	Apply
2	Understand	Assist
1	Remember	Follow

Trainer Qualification Criteria

Criteria:	Trainers must hold the ISEB Certificate in Information Security Management Principles with a minimum of 80% pass rate.

Class Room Size

Trainer to candidate ratio:	1:16