BCS Foundation Certificate in Information Security Management Principles

Version 9.0

June 2020

This professional certification is not regulated by the following United Kingdom Regulators – Ofqual, Qualification in Wales CCEA or SQA.

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

Version Number	Changes Made
V9.0 June 2020	New template format adopted, standardisation of K levels. Some areas adapted to be more appropriate for the current environment.
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 the BCS Foundation Certificate in Information Security Management Principles. Candidates are required to demonstrate their knowledge and understanding of these aspects, as specified in the learning objectives provided.

The certificate is relevant to anyone requiring an understanding of the 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.

Target Audience

The certificate is relevant to anyone requiring an understanding of 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 organisations to begin to ensure their information is protected appropriately.

Levels of Knowledge / SFIA Levels

This syllabus will provide candidates with the levels of difficulty / knowledge 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 further explained on the website www.bcs.org/levels.

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

Learning Outcomes

Candidate will be able to demonstrate knowledge and understanding of Information Security Management Principles in the following areas:

1. Knowledge of the concepts relating to information security management (confidentiality, integrity, availability, vulnerability, threats, risks, countermeasures)
2. Understanding of the relevant current legislation and regulations which impact upon information security management
3. Comprehension of the relevant current national and international standards, frameworks and organisations which facilitate the management of information security
4. Knowledge of the environments in which information security management has to operate
5. Understanding 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.

Study Format and Duration

Candidates can study for this certificate in two ways:

- Attending an accredited training course. This will require a minimum of 18 hours of study over a minimum of three days.
- Self-study. Self-study resources include online learning and recommended reading (see syllabus Reading List).

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 working knowledge of IT is 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.

Examination Format and Duration

Type	100 multiple choice questions
Duration	120 minutes
Supervised	Yes
Open Book	No (no materials can be taken into the examination room)
Pass mark	65/100 (65%)
Delivery	Digital or paper based.

Additional Time

For Candidates Requiring Reasonable Adjustments Due to a Disability.

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, then they 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

Guidelines for Accredited Training Organisations

Each major subject heading in this syllabus is assigned a percentage weighting. The purpose of this is:

1) Guidance on the proportion of content allocated to each topic area of an accredited course.
2) Guidance on the proportion of questions in the exam.

Courses do not have to follow the same order as the syllabus and additional exercises may be included, if they add value to the training course.

Question Weighting

Syllabus Area	Syllabus Weighting	Target number of questions per exam
1. Information Security Management Principles	10%	10
2. Information Risk	10%	10
3. Information Security Framework	15%	15
4. Security Lifecycle	10%	10
5. Procedural/People Security Controls	15%	15
6. Technical Security Controls	25%	25
7. Physical and Environmental Security Controls	5%	5
8. Disaster Recovery and Business Continuity Management	5%	5
9. Other Technical Aspects	5%	5
Total	**100%**	**100 Questions**

Trainer Criteria

Criteria	• Hold the BCS Information Security Management Principles Certificate • Have an in-depth knowledge of the information security standards applicable to their country of training. • 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

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 licence 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.

Syllabus

Please note that examples given throughout the syllabus, including technologies, applications, specific laws and legal issues relating to the country(s) within which a training provider operates may be mentioned and included in course material, however the examination will only test the principles to which they refer. In some cases, references may be made to these examples listed below in the examination, however detailed knowledge of their application would not be required.

Learning Objectives

1. Information Security Management Principles (10%)

Candidates will be able to:

1.1. Identify definitions, meanings and use of concepts and terms across information security management. It includes the following 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. Organisational risk appetite and risk tolerance
1.1.7. Information security policy concepts
1.1.8. The types, uses and purposes of controls
1.1.9. Defence in depth and breadth
1.1.10. Identity, authentication, authorisation and accounting (AAA) framework
1.1.11. Accountability, audit and compliance
1.1.12. Information security professionalism and ethics
1.1.13. The information security management system (ISMS) concept
1.1.14. Information assurance and information governance

1.2. Explain the need for, and the benefits of information security including:

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. Effects 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%)

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.

Candidates will be able to:

2.1. Outline the threats to and vulnerabilities of information systems, including:

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. Threats from the Dark Web and vulnerabilities of big data and the Internet of things
2.1.6. Sources of accidental threat (e.g. internal employee, trusted partner, poor software design, weak procedures and processes, managed services, social media, 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. Describe the processes for understanding and managing risk relating to information systems

2.2.1. Risk management process: 1. establish the context, 2. assessment (including identification, analysis and evaluation) 3. treatment, communication and consultation and 4. monitoring and review
2.2.2. **Strategic** options for dealing with risks and residual risk i.e. avoid/eliminate/terminate, reduce/modify, transfer/share, 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 (15%)

Candidates will be able to:

3.1. Explain how risk management should be implemented in an organisation.

3.1.1. The organisation’s management of information security

- 3.1.1.1. Information security roles in an enterprise
- 3.1.1.2. Placement in the organisation structure
- 3.1.1.3. Senior leadership team responsibilities
- 3.1.1.4. Responsibilities across the wider organisation
- 3.1.1.5. Need to take account of statutory (e.g. data protection, health & safety), regulatory (e.g. financial conduct regulations) and advisory (e.g. accounting practices, corporate governance guidelines) requirements
- 3.1.1.6. Need for, and provision of specialist information security advice and expertise
- 3.1.1.7. Creating an organisational culture of good information security practice

3.1.2. Organisational policy, standards and procedures

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

3.1.3. Information security governance

- 3.1.3.1. Review, evaluation and revision of security policy
- 3.1.3.2. Security audits and reviews
- 3.1.3.3. Checks for compliance with security policy
- 3.1.3.4. Reporting on compliance status with reference to legal and regulatory requirements, (e.g. Sarbanes Oxley, PCI DSS, data protection legislation (e.g. GDPR))
- 3.1.3.5. Compliance of contractors, third parties and sub-contractors

3.1.4. Information security implementation

- 3.1.4.1. Planning – ensuring effective programme implementation

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

3.1.5. Security incident management

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

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

3.2. Interpret general principles of law, legal jurisdiction and associated topics as they affect information security management covering 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. 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 and preservation 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 (e.g. export licences)

3.3. Describe the 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 e.g. ISA/IEC 62443 and ISO/IEC 27011
3.3.4. Certification of information security management systems to appropriate standards
– e.g. ISO/IEC 27001
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, NIST, NIS

4. Security Lifecycle (10%)

Candidates will be able to:

4.1. Demonstrate an understanding of the importance and relevance of the information lifecycle

4.2. Identify the following stages of the information lifecycle.

4.2.1. The creation and/or acquisition of the information, (e.g. through emails, letters, phone calls, etc.)
4.2.2. The publication and/or use of the information.
4.2.3. The retention, removal and/or disposal of the information.

4.3. Outline the following concepts of the design process lifecycle including essential and non-functional requirements

4.3.1. Use of architecture frameworks e.g. SABSA, TOGAF
4.3.2. Agile development i.e. DevOps, DevSecOps and potential conflict with security
4.3.3. Sharing of information by design (e.g. cloud, Office 365 etc.)
4.3.4. Service continuity and reliability

4.4. Demonstrate an understanding of the importance of appropriate technical audit and review processes, of effective change control and of configuration management

4.4.1. Methods and strategies for security testing of business systems, including vulnerability assessments and penetration testing
4.4.2. Need for correct reporting of testing and reviews
4.4.3. Verifying linkage between computer and clerical processes
4.4.4. 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

4.5. Explain the risks to security brought about by systems development and support

4.5.1. Security requirement specification
4.5.2. Security involvement in system and product assessment – including open source vs proprietary solutions
4.5.3. Security issues associated with commercial off-the-shelf systems/applications/ products
4.5.4. Importance of links with the whole business process – including clerical procedures
4.5.5. Separation of development, test and support from operational systems
4.5.6. Security of acceptance processes and security aspects in process for authorising business systems for use
4.5.7. Role of accreditation of new or modified systems as meeting their security policy
4.5.8. Change control for systems under development to maintain software integrity
4.5.9. Security issues relating to outsourcing software development
4.5.10. Preventing covert channels, Trojan code, rogue code, etc. – code verification techniques

4.5.11. Handling of security patches and non-security patches (e.g. OS upgrades)
4.5.12. Use of certified products/systems including source libraries and templates
4.5.13. Use of “Escrow” to reduce risk of loss of source code

5. Procedural/People Security Controls (15%)

Candidates will be able to:

5.1. Explain the risks to information security involving people.

5.1.1. Organisational culture of security
5.1.2. Employee, contractor and business partner awareness of the need for security
5.1.3. Security clearance and vetting
5.1.4. Role of contracts of employment
5.1.5. Need for and topics within service contracts and security undertakings
5.1.6. Rights, responsibilities, authorities and duties of individuals - codes of conduct
5.1.7. Typical topics in acceptable use policies
5.1.8. Role of segregation of duties/avoiding dependence on key individuals
5.1.9. Typical obligations on interested parties (e.g. supply chain, managed service providers, outsourced services, etc.)

5.2. Describe user access controls that may be used to manage those risks

5.2.1. Authentication and authorisation mechanisms (e.g. passwords, tokens, biometrics, multi-factor authentication, etc.) and their attributes (e.g. strength, acceptability, reliability)
5.2.2. 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.
5.2.3. Approaches to administering and reviewing access controls including role-based access, management of privileged users, management of users (joining, leaving, moving, etc.), emergency access
5.2.4. Access points – remote, local, web-based, email, etc. - and appropriate identification and authentication mechanisms
5.2.5. Information classification and protection processes, techniques and approaches

5.3. Identify the importance of appropriate training for all those involved with information

5.3.1. Purpose and role of training – need to tailor to specific needs of different interested parties (e.g. users vs. specialist vs. business manager vs. external parties)
5.3.2. Approaches to training and promoting awareness – e.g. videos, books, reports, computer based training and formal training courses
5.3.3. Sources of information, including internal and external conferences, seminars, newsgroups, trade bodies, government agencies, etc.
5.3.4. Developing positive security behaviour
5.3.5. Continual professional development and training refreshment

6. Technical Security Controls (25%)

Candidates will be able to:

6.1. Outline the technical controls that can be used to help ensure protection from Malicious Software.

6.1.1. Types of malicious software – Trojans, botnets, viruses, worms, active content (e.g. Java, Active-X, XSS), ransomware, etc.
6.1.2. Different ways systems can get infected (e.g. phishing, spear-phishing, click-bait, third party content)
6.1.3. Methods of control – internal and external, client/server, common approaches, use of good practice guides, opensource intelligence, need for regular updates, Open Web Application Security Project, etc.
6.1.4. Security by design, security by default and configuration management

6.2. Identify information security principles associated with the underlying networks and communications systems.

6.2.1. Entry points in networks and associated authentication techniques
6.2.2. Partitioning of networks to reduce risk – role of firewalls, routers, proxy servers and network boundary separation architectures
6.2.3. The role of cryptography in network security – common protocols and techniques (HTTPS, PKI, SSL/TLS, VPN, IPSec, etc.)
6.2.4. Controlling third party access (types of and reasons for) and external connections
6.2.5. Network and acceptable usage policy
6.2.6. Intrusion monitoring and detection methods and application
6.2.7. End-to-end assessment of vulnerabilities and penetration testing of networks and connections, etc.
6.2.8. Secure network management (including configuration control and the periodic mapping and management of firewalls, routers, remote access points, wireless devices, etc.)

6.3. Recognise the information security issues relating to value-added services that use the underlying networks and communications systems. This includes:

6.3.1. Securing real-time services (instant messaging, video conferencing, voice over IP, streaming, etc.)
6.3.2. Securing data exchange mechanisms e.g. e-commerce, email, internet downloads, file transfers, virtual private network (VPN), etc.
6.3.3. Protection of web servers and e-commerce applications
6.3.4. Mobile computing, home working and BYOD
6.3.5. 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

6.4. Recall 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:

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

6.5. Define the following aspects of security in information systems, including operating systems, database and file management systems, network systems and applications systems and how they apply to the IT infrastructure. This includes:

6.5.1. Security information and event monitoring (SIEM)
6.5.2. Separation of systems to reduce risk
6.5.3. Conformance with security policy, standards and guidelines
6.5.4. Access control lists and roles, including control of privileged access
6.5.5. Correctness of input and ongoing correctness of all stored data including parameters for all generalised software
6.5.6. Visualisation and modelling of threats and attacks
6.5.7. Recovery capability, including back-up and audit trails
6.5.8. Intrusion monitoring, detection methods and application
6.5.9. Installation baseline controls to secure systems and applications - dangers of default settings
6.5.10. Configuration management and operational change control
6.5.11. The need to protect system documentation and promote security documentation within the organisation, within partner organisations and within managed service and outsourced operations

7. Physical and Environmental Security Controls (5%)

Candidates will be able to:

7.1. Outline the physical aspects of security available in multi-layered defences and explain how 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.

7.1.1. General controls and monitoring of access to and protection of physical sites, offices, secure areas, cabinets and rooms
7.1.2. Protection of IT equipment – servers, routers, switches, printers, etc.
7.1.3. Protection of non-IT equipment, power supplies, cabling, etc.
7.1.4. Need for processes to handle intruder alerts, deliberate or accidental physical events, etc.
7.1.5. Clear screen and desk policy

7.1.6. Moving property on and off-site
7.1.7. Procedures for secure disposal of documents, equipment, storage devices, etc.
7.1.8. Procedures for the disposal of equipment with digital-data retention facilities e.g. multi-function devices, photocopiers, network printers, etc.
7.1.9. Security requirements in delivery and loading areas

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

Candidates will be able to:

8.1. Describe (K1/2) the differences between and the need for business continuity and disaster recovery.

8.1.1. Relationship with risk assessment and impact analysis
8.1.2. Resilience of systems and infrastructure
8.1.3. Approaches to writing and implementing plans
8.1.4. Need for documentation, maintenance and testing of plans
8.1.5. Need for links to managed service provision and outsourcing
8.1.6. Need for secure off-site storage of vital material
8.1.7. Need to involve personnel, suppliers, IT systems providers, etc.
8.1.8. Relationship with security incident management
8.1.9. Compliance with standards - ISO 22300 series or other relevant international standards

9. Other Technical Aspects (5%)

Candidates will be able to:

9.1. Demonstrate understanding 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, including intelligence sharing platforms (e.g. CiSP)
9.1.2. Legal and regulatory guidelines for disclosures, investigations, forensic readiness and evidence preservation
9.1.3. Need for relations with law enforcement, including specialist computer crime units and security advice
9.1.4. Issues when buying-in forensics and investigative support from third parties

9.2. Describe 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)

9.2.5. Use by individuals of encryption facilities within applications (e.g. WhatsApp, VPN, certificates)

Recommended Reading List

Title	Information Security Management Principles 3rd edition
Authors	David Alexander, Amanda Finch, David Sutton, Andy Taylor
Publisher:	BCS, Learning and Development Limited 2020
Publication:	January 2020 – 3rd edition
ISBN:	978-1-780175-18-8

Syllabus References

- COBIT Framework Framework for IT Governance and Control
- ITIL - IT Infrastructure for Service Management
- Chartered institute for Information Security (CIISec)
- 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
- BCS Cyber Crime Forensics Specialist Group
- BCS Information Risk Management and Assurance Specialist Group
- EU Regulation 679 General Data Protection Regulation (https://gdpr-info.eu/)

Common Standards

- ISO 31000 – Risk Management Principles and Guidelines
- ISO 31010 – Risk Management – Risk Assessment Techniques
- COSO – Enterprise Risk Management Integrated Framework
- OCEG Red Book - A Governance, Risk and Compliance Capability Model
- ISO Guide 73 - Definitions of generic terms related to Risk Management
- ISO 27005 - Guidelines for information security risk management
- ISO 27000 - Information technology – Security techniques – Information security management systems – Fundamentals and vocabulary
- ISO 27001 - Specification for an Information Security Management System
- ISO 27002 - Information technology – Security techniques – Code of Practice for Information Security Management (this replaces BS 17799)
- ISO 22301 - Security and resilience — Business continuity management systems — Requirements

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.