

**Qualification Specification for the**

**Knowledge Modules that form part of the BCS Level 4 Cyber Security Technologist Apprenticeship**

**BCS Level 4 Certificate in Cyber Security Introduction**

**BCS Level 4 Certificate in Network and Digital Communications**

**Theory**

**BCS Level 4 Certificate in Security Case Development and Design**

**Good Practice**

**BCS Level 4 Certificate in Security Technology Building Blocks**

**BCS Level 4 Certificate in Employment of Cryptography**

**BCS Level 4 Award in Risk Assessment**

**BCS Level 4 Certificate in Governance, Organisation, Law, Regulation and Regulation and Standards**

**Version 3.0**

**February 2018**

**Contents**

**1. About BCS 3**

**2. Equal Opportunities 3**

**3. Introduction to the Qualification 3**

3.1 Qualification summary 3

3.2 Purpose of the qualifications 4

3.3 Structure of the qualifications 4

3.4 Prior learning 5

3.5 Learner progression 6

**4. Units 7**

4.1 Guidance on the qualifications’ content 7

4.2 Learning Outcomes and Assessment Criteria 8

**5. Assessment 52**

5.1 Summary of assessment methods 52

5.2 Availability of assessments 52

5.3 Grading 52

5.4 Externally assessed units 52

5.5 Specimen assessment materials 52

5.6 Support materials 52

5.7 Access to Assessment 53

**6. Contact Points 53**

**1. About BCS**

Our mission as BCS, The Chartered Institute for IT, is to enable the information society. We promote wider social and economic progress through the advancement of information technology, science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, design new curricula, shape public policy and inform the public.

Our vision is to be a world class organisation for IT. Our 70,000 strong membership includes practitioners, businesses, academics and students in the UK and internationally. We deliver a range of professional development tools for practitioners and employees. As a leading IT qualification body, we offer a range of widely recognised qualifications.

**2. Equal Opportunities**

BCS wishes to ensure good practice in the area of Equal Opportunity. Equality of opportunity extends to all aspects for the provision of BCS qualifications.

**3. Introduction to the Qualification**

**3.1 Qualification summary**

|  |  |  |
| --- | --- | --- |
| **Qualification Title** | **QAN** | **Accreditation**  **Start** |
| 1. BCS Level 4 Certificate in Cyber Security  Introduction. | **603/0830/8** | **07/12/2016** |
| 2. BCS Level 4 Certificate in Network and  Digital Communications Theory. | **603/0703/1** | **02/11/2016** |
| 3. BCS Level 4 Certificate in Security Case  Development and Design Good Practice. | **603/0904/0** | **13/12/2016** |
| 4. BCS Level 4 Certificate in Security  Technology Building Blocks. | **603/0884/9** | **12/12/2016** |
| 5. BCS Level 4 Certificate in Employment of  Cryptography. | **603/0892/8** | **13/12/2016** |
| 6. BCS Level 4 Award in Risk Assessment. | **603/0866/7** | **09/12/2016** |
| 7. BCS Level 4 Certificate in Governance,  Organisation, Law, Regulation and  Standards. | **603/0855/2** | **08/12/2016** |

The Level 4 Cyber Security Technologist Apprenticeship has a choice of 2 learning pathways: The ‘Technologist’ learning pathway, which requires the completion of knowledge modules 1 through to 5 and the ‘Risk Analyst’ learning pathway, which requires the completion of knowledge modules 1, 6 and 7.

The knowledge modules have been developed based on the requirements set out in the Standard issued by the Tech Partnership and approved by the Government, details of which can be located in the Assessment Plan ([Click here)](https://www.thetechpartnership.com/globalassets/pdfs/apprenticeship-standards/cyber-security-technologist/app_assessmentplan_cybersecuritytechnologist.pdf) and Occupational Brief ([Click here)](https://www.thetechpartnership.com/globalassets/pdfs/apprenticeship-standards/cyber-security-technologist/app_occupationalbrief_cybersecuritytechnologist.pdf) documents.

No vendor or professional qualifications have been identified that would exempt these Knowledge Modules.

All BCS qualifications are subject to our quality assurance and validation process. This ensures that new and revised qualifications are fit for purpose. Qualifications are reviewed to ensure the alignment of the qualification with agreed design principles, regulatory requirements and to ensure accuracy and consistency across units and qualifications. Through our quality assurance and validation process, we ensure the qualification, its units and assessments are fit for purpose and can be delivered efficiently and reasonably by Training Providers.

**3.2 Purpose of the qualifications**

The qualifications are designed for apprentices enrolled on the Level 4 Cyber Security Technologist Digital IT Apprenticeship, to provide them with the technical knowledge and understanding they require for their role detailed below:

*The primary role of a Cyber Security Technologist is to apply an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organisations systems and people. Those focused on the technical side work on areas such as security design & architecture, security testing, investigations & response. Those focussed on the risk analysis side focus on areas such as operations, risk, governance & compliance. Whether focussed on the technical or risk analysis side, all people in this occupation work to achieve required security outcomes in a legal and regulatory context in all parts of the economy. They develop and apply practical knowledge of information security to deliver solutions that fulfil an organisation’s requirements.*

**3.3 Structure of the qualifications**

This document covers the following qualifications which are used towards the Level

4 Cyber Security Technologist Apprenticeship. The qualifications can be taken in any order; however, it is recommended that they be completed in the following sequence:

Technologist Learning Pathway - Knowledge Modules 1,2,3,4,5

Risk Analysis Learning Pathway - Knowledge Modules 1,6,7

|  |  |
| --- | --- |
| Qualification Level 4 Cyber Security Technologist Apprenticeship | |
| Knowledge  descriptor (the  holder…) | Apprentices will develop an understanding and be able to  have factual, procedural and theoretical knowledge of fundamental Cyber Security theory, techniques, risk analysis and law. |
| Skills  descriptor (the  holder can…) | Apprentices undertaking the ‘Technologist’ learning pathway will develop skills and be able to demonstrate the following topics: Showing an understanding of basic networks and security components; data protocols; how to build a security case; good design practice; common security architectures; show an appreciation for reputable security architectures (to incorporate hardware and software components); security controls and threats; basic cryptography and key legal issues.  Apprentices undertaking the ‘Risk Analysis’ learning pathway will develop skills and be able to demonstrate an understanding of Cyber Risk assessment methodologies; threats; threat trends; audit and assurance; cryptography and its main techniques; the significance of key management and appreciate the associated legal standards, regulations and ethical standards relevant to cyber security.  Apprentices should be able to demonstrate: logical and creative thinking; analytical and problem solving skills; an ability to work independently and to take responsibility using their own initiative; show an ability to work with a range of internal and external people; have an ability to communicate effectively in a variety of situations and maintain a productive, professional and secure working environment. |

**3.4 Prior learning**

Individual employers will set the selection criteria for enrolment onto the Apprenticeship, but this is likely to include five GCSEs, (especially English, Mathematics and a Science or Technology subject); a relevant Level 3

Apprenticeship; other relevant qualifications and experience; or an aptitude test with a focus on IT skills.

**3.5 Learner progression**

This document covers the qualifications that are part of the Level 4 Cyber Security Technologist apprenticeship. The qualifications must be completed to allow the apprentice to progress onto the end-point assessment, detailed below.

*The final end-point assessment is completed in the last few months of the apprenticeship. It is based on:*

• *a portfolio – produced towards the end of the apprenticeship, containing evidence from real work projects which have been completed during the apprenticeship, usually towards the end and which, taken together, cover the totality of the standard and which is assessed as part of the end-point assessment*

• *a project - giving the apprentice the opportunity to undertake a business-related project over a one-week period away from the day to day workplace*

• *an employer reference*

• *a structured interview with an assessor - exploring what has been produced in the portfolio and the project, as well as looking at how it has been produced*

*An independent assessor will evaluate each element of the end-point assessment and will then decide whether to award successful apprentices with a pass, a merit or a distinction.*

**4. Units**

**4.1 Guidance on the qualifications’ content**

The content for each qualification has been developed based on the criteria set out in the Occupational Brief.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Qualification Title** | **TQT (Guided Learning + Direct**  **Study + Assessment)** |  |
| 1. BCS Level 4 Certificate in Cyber  Security Introduction. | 199 (132h + 66h + 1h) |
| 2. BCS Level 4 Certificate in Network  and Digital Communications Theory. | 124 (82h + 41h + 1h) |
| 3. BCS Level 4 Certificate in Security  Case Development and Design  Good Practice. | 132 (75h + 56h +1h) |
| 4. BCS Level 4 Certificate in Security  Technology Building Blocks. | 125 (83h + 41h + 1h) |
| 5. BCS Level 4 Certificate in  Employment of Cryptography. | 125 (83h + 41h + 1h) |
| 6. BCS Level 4 Award in Risk  Assessment. | 58 (38h + 19h +1h) |
| 7. BCS Level 4 Certificate in  Governance, Organisation, Law, Regulation and Standards. | 128 (42h + 85h + 1h) |

**4.2 Learning Outcomes and Assessment Criteria**

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Cyber Security Introduction. | Describe and explain why information and  cyber security are important to business and to society. | Describe and explain the evaluation of information assets  and the criticality to a business. |
| Describe and explain how cyber security can have a direct  impact on the reputation and continuing success of a business. |
| Describe and explain how the cyber security of businesses  contributes to the overall economy and security of the society in which it operates. |
| Recall, relate and explain the terminology and basic concepts of cyber security. | Recall and explain key terminology. This could include, but not be limited to:  • Security  • Identity  • Authentication  • Non-repudiation  • Confidentiality  • Integrity  • Availability  • Threat  • Vulnerability  • Risk and hazard |

|  |  |  |
| --- | --- | --- |
|  |  | Describe what security is, fundamentally, by explaining:  • How the concepts of threat, hazard and vulnerability relate to each other and lead to risk.  • The inherent asymmetric nature of cyber security threats. |
| Describe and explain:  • What risk is  • How risks are usually quantified (by likelihood and relative impact)  • The use of at least one commonly used tool for risk management; for example, but not limited to, a risk register. |
| Describe typical threats, threat actors and hazards in terms  of capability, opportunity and motive using examples that may concern an organisation. These may include, but not be limited to:  • Profiling techniques  • Relating these threat descriptions to example security objectives |
| Describe and explain how an organisation balances  business drivers and costs with the outcome and recommendations of a cyber security risk assessment. Apprentices will also consider the wider business risk context using, as an example, but not limited to: a business impact assessment (BIA). |

Explain the concept of security assurance and demonstrate how it can be delivered.

Recall, describe and explain security assurance concepts and how these might be applied at different stages in the lifecycle of a system; including, but not limited to:

• The difference between ‘trusted’ and ‘trustworthy’

• The purpose of security assurance

• The main approaches to:

o Assurance

o Intrinsic and extrinsic

o Design and implementation

o Operational policy & process

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Cyber Security Introduction.  **(continued)** |  | Describe and explain the way security assurance works in  practice regarding the concepts. |
| Describe and explain what penetration testing is and how it  contributes to security assurance; for example, but not limited to ‘ethical hacking’. Apprentices will also show an understanding of the differences between internal and external penetration testing. |
| Describe at least one current system of extrinsic assurance,  explaining the benefits and limitations. For example, but not limited to:  • Security testing  • Supply chain assurance  • Common criteria |
| Describe at least two ways an organisation can provide  intrinsic assurance. |
| Describe and explain how security  objectives can be used to build a security case. | Explain how to develop and justify security objectives for a  proposed business solution. |
| Describe how security objectives might be used to define  information and infrastructure assets in representative business scenarios. |
| Explain how security objectives might be justified, taking  account of the value of the assets, by understanding the importance and relative priorities in the different scenarios. |

|  |  |  |
| --- | --- | --- |
|  |  | Explain how analysis of security objectives leads to an  expression of security requirements and how this assists both with the building of a security case and in the development of the new system. |
| Demonstrate and explain how basic security  concepts can be applied to typical information and communications technology (ICT) cyber infrastructures. | Show an understanding of common vulnerabilities in  computer networks and systems. This may include, but not be limited to, non-secure coding and unprotected networks. |
| Describe the fundamental building blocks of:  • Infrastructure elements; including, but not limited to:  o Firewalls  o Routers  o Switches  o Hubs  o Storage  o Transmission.  • Typical architectures of computers, networks and the  Internet; including, but not limited to:  o Server/ client  o Hub/spoke  o Non-virtual/ virtual. |

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Cyber Security Introduction.  **(continued)** | Explain and demonstrate an understanding  of common attack techniques and sources of threat. | Describe and explain the main types of attack techniques.  For each type of attack, apprentices should illustrate the main features of how they work and suggest where and when they may be effective.  • Current attack types may include, but not be limited to:  o Phishing  o Social engineering  o Malware  o Network interception  • Blended techniques may include, but not be limited to:  o Advanced persistent threat (APT) o Denial of service (DoS and DDoS) o Information theft and ransomware. |
| Describe the role of human behaviour in cyber security,  including an ability to:  • Explain the term ‘insider threat’  • Explain an organisation’s ‘cyber security culture’ and describe some features that may characterise it. Apprentices should also show an understanding of how this cyber security culture may contribute to security risk. |

|  |  |  |
| --- | --- | --- |
|  |  | Explain how an attack technique combines with motive and  opportunity to become a threat. Apprentices should also illustrate how attack techniques are developed and why they are continuously changing. |
| Describe typical hazards and how these may achieve the  same outcome as an attack. For example, but not limited to, flood and fire. |
| Describe, solve and explain ways to defend against the main attack techniques. | Describe ways to defend against attack techniques by considering the different ways in which controls may be used; including, but not limited to:  • Deter, protect, detect and react  • Preventative, directive, detective and corrective  • Physical, procedural (people) and technical  • An attack chain |
| Recall, describe and explain the legal,  regulatory, information security and ethical standards relevant to the cyber community. | Describe the appropriate and applicable cyber security  standards, regulations and their consequences for at least two sectors, comparing their differences. Examples of sectors may include, but not be limited to:  • Government  • Public sector  • Charitable  • Finance  • Petrochemical / process control. |
| Describe and explain the role of criminal law, contract law  and other related sources of legal and regulatory control. |

Describe and explain the benefits, costs and main motives

for the uptake of significant security standards; including, but not limited to:

• Common Criteria

• PCI-DSS

• FIPS-140-2

• CESG Assisted products (CAPS)

• COBIT

|  |  |  |
| --- | --- | --- |
|  |  | Describe and explain the main features and implications of  laws and regulations that affect organisations, systems and users in the UK. Key areas to consider are:  • The main UK laws that are relevant to cyber security issues, including legal requirements that affect individuals and organisations. Examples could include, but not be limited to:  o The Computer Misuse Act  o The Data Protection Act (DPA)  o The Human Rights Act  • The international laws and regulations that affect organisations, systems and users in the UK covering the movement of data and equipment across international borders and between jurisdictions; including, but not limited to:  o The Digital Millennium Act  o International Traffic in Arms Regulations (ITAR)  o Harbour (Safe Harbour)  o The Patriot Act  o General Data Protection Regulations (GDPR)  o The Network and Information Security Directive  (NIS)  • The legal responsibilities of system users and how these may be communicated effectively |
| Describe and explain the ethical responsibilities of a cyber- security professional, by reference to at least one generally recognised and relevant professional body influential in the UK. |

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Cyber Security Introduction.  **(continued)** | Discover and explain the concept and  practice of keeping up with the threat landscape (horizon scanning). | Describe and know how to apply relevant techniques for  horizon scanning and can:  • Recall, discover and explain the relative merits of at least three external sources of horizon scanning. These may include, but not be limited to:  o Market trend reports  o Academic research papers  o Professional journals o Hacker conferences o Online  o Government sponsored sources; including, but not limited to: The National Cyber Security Centre (NCSC), CiSP and CertUK  • Describe and explain the value of using a diversity of sources  • Explain the horizon scanning technique, using current examples from sources relevant to cyber security in the UK  • Determine the reliability and trustworthiness of different sources. |
| Describe and explain the application of at least one  technique to identify trends in research and illustrate with an example. |
| Describe and explain future trends in cyber security. | Describe and explain the significance of some identified trends in cyber security. |

Explain the value and risk of this analysis.

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Network and Digital Communications Theory | Describe and explain the common networks  in use and their associated data formats, protocols and related performance issues. | Describe data formats and protocols in current use. |
| Explain features of network protocols in widespread use on  the Internet. Including, but not limited to:  • HTTPS  • HTTP  • SMTP  • SNMP  • TCP  • UDP  • IP |
| Identify network failure modes and reasons why networks  ‘hang’. |
| Describe approaches to error control in a network. |
| Explain network layer models and then  contrast their differences. | Explain features of the following layered network models:  • TCP/IP Reference Model  • OSI 7 Layer Model |
| Compare the differences between the following physical layer categories and datalink layer protocols:  • Physical Layers (including, but not limited to: Wireless, Fibre, Wired)  • Data Link Layer (including, but not limited to: Ethernet  [802.3], Wireless LAN [802.11], Bluetooth) |

|  |  |  |
| --- | --- | --- |
|  | Describe and explain network routing  protocols. | Describe current network routing protocols in use; including, but not limited to:  • RIP/RIP2  • RIP-NG  • OSPF  • OSPFv2  • OSPFv3 |
| Compare the differences between static and dynamic routing. |
| Describe and explain the factors that affect  network performance. | Demonstrate the relationship between factors that affect  network performance; including, but not limited to:  • Bandwidth  • Number of users  • Nature  • Contention |
| Explain methods of improving network performance; such as,  but not limited to: traffic shaping and architecture. |

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Security Case Development and Design Good Practice | Describe and explain recognised IT Security  Design Principles and demonstrate their application within IT systems and software. | Demonstrate the importance of keeping IT systems simple, whilst meeting business and security needs. |
| Describe the application and features of core IT Security  Design Principles, including but not limited to:  • Least privilege  • Economy of mechanism  • Defence in depth (complete mediation)  • Human factors - psychological acceptability  • Fail-safe defaults  • Open design  • Separation of privileges  • Least common mechanism |
| Explain the following features of the Trustworthy Software  Initiative (TSI):  • Safety  • Reliability  • Availability  • Resilience  • Security |
| Compare TSI and IT Security Design Principles and explain their commonalities. |

|  |  |  |
| --- | --- | --- |
|  | Describe and illustrate common security  architectures that incorporate hardware and software components. | Demonstrate the difference between enterprise architecture  and security architecture, and explain where their physical and logical boundaries may exist. |
| Compare features of common security architectures;  including, but not limited to:  • SABSA  • Zachman Framework  • TOGAF  • CISCO and the NIST Cyber Security Framework |
| Relate how national bodies such as CESG, FIPS, NIST and GCHQ provide guidance and information to public and private sector organisations in the following areas:  • IT Security policies  • IT Security architectural patterns/ frameworks  • White papers  • National strategies on cyber security |
| Describe and explain the Common Criteria  Protection Profile for a security component. | Explain the purpose and features of the Common Criteria  evaluation model, including and not limited to:  • Common criteria – their application and uses  • Target of Evaluation (TOE)  • Protection profile  • Security target  • EALs  • The process of specification, implementation and evaluation for certified products and systems |

Describe how Common Criteria may be used to feed into a security case.

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Security Case Development and Design Good Practice  **(continued)** | Construct a Security Case for a system. | Produce a Security Case for a known system, including:  • A clear definition of the objectives of the case: who, what, where, why and when  • Threats that are likely to exist against the target system  • Known attack profiles likely to be used by malicious individuals  • Risks to the system, measured in probabilities (very likely, likely and unlikely)  • Potential impact (major, moderate, minor)  • Potential severity (high, medium, low)  • Physical protection measures that may be required; for example, but not limited to:  o CCTV/ alarms  o Backups  o Cabinets |

Considering the Security Case, interpret what security measures should apply:

• Technical protection measures using hardware devices; including, but not limited to:

o Firewalls

o Routers

o SIEM

• Software components; including, but not limited to:

o Access rights

o Anti-virus

o Scanners

• Implementation strategies for a proposed solution;

including, but not limited to:

o Constraints

o Dependencies

o Cost benefit analysis

• IT security policies that may be needed as part of the security case; including, but not limited to: backups and data protection

• Where applicable, complete a test plan to include descriptors and expected results

|  |  |  |
| --- | --- | --- |
|  |  | Considering the Security Case, indicate examples of:  • Applicable processes that may need to be implemented by personnel or systems  • Overview of legal responsibilities, where applicable  • Staff training that maybe required for the new measures  • Future proofing  • Alternative solutions to the case for due consideration.  For example, but not limited to:  o OTS solutions  o Third-party contracts  o Complete software solutions |
| Describe (using software applications, hardware components and examples), how threats evolve over time to respond to system security hardening. |

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Security Technology Building Blocks | Describe and explain the tools and methods  commonly employed to protect hosts, application and system software and stored data from a range of threats, as well as the responsibilities of computer users in keeping their systems secure. | Describe computer and data authentication methods in  current use. |
| Describe methods employed to protect and secure data held  on the host. Indicative areas of study can include, but are not limited to:  • Types of authentication  • Access control  • Physical security  • TCP ports  • Disk encryption  • Checksums |
| Explain the importance of and the methods employed to keep  the software environment healthy and up to date. Indicative areas of study can include, but are not limited to:  • Zero day attacks  • Operating system and application updates  • Antivirus updates |
| Describe the responsibilities of the user for PC protection, in  keeping their PC and its data secure from threats. For example, but not limited to:  • Social engineering  • Software updates  • Password management  • Internet etiquette |

|  |  |  |
| --- | --- | --- |
|  | Identify and select appropriate technologies  and techniques necessary for the defence of computer networks, their hosts and their users. | Describe the hardware components available for network  protection and their purpose and demonstrate the ability to select the appropriate system for a given task. Indicative technologies can include, but are not limited to:  • Firewalls and DPI  • Application proxies  • IDS vs. IPS  • RADIUS  • AAA |
| Describe the policy based methods available for network  protection and explain their purpose. For example, but not limited to:  • QoS  • Cross-domain components  • DMZ  • Gateways  • Routing  • Traffic prioritisation  • Anomaly & misuse detection |

|  |  |  |
| --- | --- | --- |
|  |  | Describe methods available for the protection of data whist in  transit and demonstrate the ability to select from a range of current technologies and appropriate methods for the protection of data as it crosses arbitrary networks. Indicative areas of study are secure Internet transaction technologies; including but not limited to:  • IPSec  • TLS  • SSH  • Negotiation  • Cryptography  • Key management |
| Describe the responsibilities of network administrators and  approaches available for the management of security in the network. Apprentices should also explain the necessity for network and server configuration and maintenance, as well as available methods. Including but not limited to:  • Network segregation  • Security issues for common client & server configuration  • Performance management  • Staff training  • File and user permissions  • Password management |

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Security Technology Building Blocks  **(continued)** | Identify and select appropriate technologies  and techniques necessary for the defence of software, applications and the data held on hosts | Describe frameworks and processes available for secure  application development and apply appropriate security processes to the software development lifecycle. Typical areas of study can include, but are not limited to:  • OWASP Top 10 awareness for web application development  • Common Weakness Enumeration guideline awareness for general software development  • National Cyber Security Centre (NCSC) guidelines  • Secure SDLC |
| Describe IDAM Tools and systems available for application  and data protection, and how these can be applied to manage application security. For example, but not limited to:  • Identity management systems and protocols  • Tickets  • Tokens  • Session  • Multi factor authentication  • Access control  • Definitions (identity, authentication, authorisation, Bell- LaPadula model) |

|  |  |  |
| --- | --- | --- |
|  |  | Describe application firewalls and reverse proxies and  demonstrate the ability to select from a range of current technologies or appropriate tools to enhance the protection of data as it is captured and returned by applications. Indicative technologies can include, but are not limited to:  • Application sensors  • Application firewalls  • Proxies and reverse proxies  • Application level security logging and monitoring  • Log configuration |
| Describe database security mechanisms, including the responsibility of encryption in protecting user data; show the necessity for securing data at rest and describe different ways this can be done using database applications. For example, but not limited to:  • Field vs record based encryption  • SQL security  • Backup security  • Database access control |
| Select technologies and techniques  necessary for the management of a secure computer system and describe risk mitigation techniques that can be applied at | Correctly apply risk mitigation techniques; such as, but not  limited to:  • Threat modelling (example STRIDE)  • Security controls (SANS Top 20, NIST 800-53, GPG  13) |

|  |  |  |
| --- | --- | --- |
|  | the host, network or application layer to  secure computer systems. | Apply security mechanisms as they relate to the CIA Triad;  particularly, how to select security mechanisms to implement all three into a computer system. Indicative areas of study can include, but are not limited to:  • Confidentiality (select layers for encryption)  • Integrity (validating the integrity of data transmissions)  • Availability (load balancing, proxies, anti DDOS, WAF) |
| Explain accreditation and assurance processes that relate to the application of security technology. Apprentices will demonstrate the ability to apply supplier, software and component assurance and accreditation processes (first introduced in the Cyber Security Technologist, Knowledge Module 2 and described in sections 1 to 3 above). Indicative study can include, but is not limited to:  • Penetration testing  • Vulnerability assessment and threat intelligence  • ISMS and standards role in accreditation and supplier assurance (ISO27001, PCI DSS, common criteria, product assurance)  • Software code review (SAST, DAST, IAST, reviews) |

Describe Security Technology Solutions in terms of their benefits and limitations and explain strengths, weakness and applicability of security technology as described in section 1 to 3 above. Typical areas of study can include, but are not limited to:

• Automation vs. manual validation of security

• Open source vs. closed source solutions

• On premises vs. off premises solutions (cloud based, private, hybrid and public)

• Iterative vs. Waterfall projects implication on security engineering

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Employment of Cryptography | Describe the technology of cryptography  and name the available techniques, limitations and problems commonly encountered. | Describe cryptographic techniques and state their limitations.  For example, but not limited to:  • Ciphertext vs. Plaintext  • Ciphers  • Cryptographic techniques  • Key length vs. Security  • Hashing  • Digital signatures  • Attacks |
| Describe the main features of symmetric cryptosystems, PK  cryptosystems and key exchange. |
| Show where the various cryptographic techniques may be  employed to secure data and systems. For example, but not limited to:  • Password verification  • Digital signatures  • VPNs  • Tunnelling  • Encapsulating & carrier protocols  • IPsec |

|  |  |  |
| --- | --- | --- |
|  |  | Show how poorly applied cryptography can become a threat  vector. Indicative areas of study include, but are not limited to:  • ECB mode  • Collision attacks  • Algorithm problems  • Key management problems  • Random number generation problems |
| Explain the significance and role of entropy in cryptography and discuss security problems associated with entropy. |
| Explain the deployment of cryptographic  systems in a range of common public technologies; in the protection of data and networked systems and discuss issues faced in their deployment and updating. | Explain the significance of key management as it relates to  controls, lifecycle and governance. |
| Describe the role of cryptography in a range of common  public systems. For example, but not limited to:  • Mobile telecommunications  • Secure card payments  • Cyber applications  • Video broadcasting  • Private and home user considerations |
| Describe the role of cryptography as it applies to data on hard  disks or in transit. For example, but not limited to:  • Secure Internet transaction technologies  • Data at rest  • Open vs closed source |

|  |  |  |
| --- | --- | --- |
|  |  | List some of the practical issues encountered in implementing  cryptography. Indicative areas may include, but not be limited to:  • Performance considerations  • Storage of keys  • Security clearance of custodians  • Historical consideration of broken cryptographic systems  • Theoretical vs practical security  • Kerckhoff’s principle |
| Explain the practical issues faced when updating  cryptographic techniques. For example, but not limited to:  • Vulnerability analysis  • Intelligence sources  • General understanding of validation processes  • Patching process and testing |

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Employment of Cryptography  **(continued)** | Discuss legal issues relevant to  cryptography (particularly when crossing national borders) and describe UK, EU and US export control of cryptography and the Wassenaar Arrangement. | List the regulatory frameworks in place in different  jurisdictions, covering such topics as:  • International Traffic in Arms Regulations  • DPA  • FoI  • The Combined Code  • Sarbanes-Oxley and their areas of governance  • RIPA 2000  • Key escrow  • International Data Encryption Algorithm (IDEA) |
| Describe some of the legal issues related to cryptography  with respect to national borders. |
| List a range of resources available to obtain advice concerning cryptography and security. For example, but not limited to:  • CAVP  • CVE lists  • Open vs. closed reviews  • ISO  • OWASP  • SANS  • NIST  • NCSC |

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Award in Risk  Assessment | Describe and explain how to manage  information security, cyber risks and threats efficiently and effectively within an organisation. | Understand the principles and terminology of risk; for  example, but not limited to:  • Probability  • Likelihood  • Threat  • Vulnerability  • Impact  • Threat actor  • Risk owner |
| Understand and describe the five key steps in risk  management:  • Identify assets  • Identify threats and vulnerabilities  • Assess the impact of threats and vulnerabilities on an organisation  • Identify ways to manage those threats and vulnerabilities  • Monitor and report on risk management action |
| Discuss qualitative and quantitative approaches to risk  assessment; including, but not limited to:  • Quantitative approaches (such as loss expectancy approaches (SLE/ARO))  • Quantitative scalar approaches (such as  High/Medium/Low) |

|  |  |  |
| --- | --- | --- |
|  |  | Illustrate how the results of an assessment can be presented;  for example, but not limited to:  • Financial impact  • Dashboards  • Heat maps  • RAG. |
| Demonstrate an understanding of the  differences of threats and vulnerabilities. | Define and state the differences between:  • Threat  • Vulnerability  • Exploit  • Attack |
| Describe and explain the following:  • Categories of threats  • The concept of a threat lifecycle  • The use of threat intelligence in an organisation  • The uses of attribution |
| Discuss vulnerabilities, especially those relating to people and  staff. Apprentices will understand how they can be exploited to attack an organisation; including, but not limited to:  • Phishing  • Social engineering  • Blended attacks |

|  |  |  |
| --- | --- | --- |
|  |  | Describe common methods for finding vulnerabilities; for  example, but not limited to:  • Penetration testing  • Phishing simulators  • Social engineering attacks |
| Explore factors relating to the standards surrounding cyber risk assessment. | Explain that risk assessment can be carried out using several methodologies or frameworks, but that it is better to select  one methodology or framework for consistent and comparable results. |
| List the common risk assessment methodologies or  frameworks; including, but not limited to:  • ISO/IEC 27005  • NIST Risk Management Framework  • OCTAVE  • FAIR |
| Compare common risk methodologies/frameworks;  highlighting similarities and differences. |
| Demonstrate how to select and then apply a risk  methodology/framework in an organisation. |

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Award in Risk  Assessment  **(continued)** | Describe and explain how to apply a risk  assessment methodology in an organisation. | Demonstrate how a risk assessment methodology/framework  can be applied in an organisation to one or more of the following:  • Systems  • Applications  • Networks and information |
| Illustrate how vulnerabilities can be identified using a range of  tools and techniques; including, but not limited to: research and technical. |
| Compare approaches to treating risk; for example, but not  limited to:  • Accept  • Transfer  • Avoid  • Mitigate  Apprentices should also supply examples of how these approaches to treating risk can be achieved in practice; including, but not limited to: applying technical security controls to protect a system. |
| Discuss the role of risk owner and compare that role with other stakeholders. |

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Governance, Organisation, Law, Regulation and Standards | Explain the need for appropriate  governance, organisational structure, roles, policies, standards and guidelines for cyber and information security, and how they work together to deliver identified security outcomes. | Explain why governance, organisational structure, roles,  policies, standards and guidelines are needed to manage information security by describing how an organisation can:  • Align information security with business strategy;  • Manage risks appropriately;  • Manage resources efficiently and effectively;  • Measure performance;  • Deliver value by optimising information security investments. |

Describe a model information security management structure by explaining the roles and purposes of:

• Governance bodies:

o o the Main Board;

o the Risk Management Committee;

o the Information Security Management Board.

• Governance roles:

o the Main Board;

o executives;

o audit;

o information security.

• Management planning:

o strategic direction; o objectives setting; o risk management;

o responsible resource use.

• Accountability and responsibility.

• Appropriate business fit for security - ensuring security aligns with organisational objectives, risk environment and culture.

|  |  |  |
| --- | --- | --- |
|  |  | Understand and explain how the various elements within an  information security management structure operate together to deliver the required security outcomes using the concepts of:  • Ownership;  o risk;  o asset;  o process ownership.  • Delegation.  • Custodianship. |
| Describe how organisations can use the elements below to  integrate information security into the overall corporate governance and application development process, ensuring effective delivery of security outcomes:  • The change management process.  • Embedding security into project management practices. |
| Recognise how legislation and regulation can be  implemented in a manner that meets specific, local information security risks:  • Ensuring appropriate connections between legislation, regulation, policy, risk management and project management. |

|  |  |  |
| --- | --- | --- |
|  | Explain how an organisation’s security  policies, standards and governance are supported by provisioning and access rights (e.g. how identity and access management are implemented and maintained for a database, application or physical access control system). | Describe how effective management of identity provisioning  and access rights support an organisation’s security policies,  standards and governance via:  • Password management;  • Role based access control (RBAC);  • The principle of ‘least privilege’;  • Privileged access management;  • Principles of identity access management for access to databases, applications and physical environments;  • Physical access control tools:  o swipe cards.  o PINs.  o biometrics. |
| Describe how cyber security policies and  procedures are used in different organisational environments and affect individuals and organisations. | Describe an organisational environment and the factors and  forces that shape it through:  • General environment, task environment and internal environment.  • The components of an internal environment:  o management;  o employees;  o shareholders;  o representative bodies.  • The major forces in the external environment:  o political;  o economic;  o technological;  o socio-economic;  o legal and regulatory. |

|  |  |  |
| --- | --- | --- |
|  |  | Explain how an organisation's type can affect the way it  manages information security and how internal and external forces impact on security management in the following types of organisations:  • Central government;  • Financial services;  • Healthcare;  • Aerospace and defence;  • Utilities;  • Social services. |
|  | Describe the impact of the following regulations on the  associated organisations:  • HIPAA (healthcare);  • Sarbanes-Oxley (Listed companies with US presence);  • Basel III (international finance);  • PCI-DSS (all businesses that use credit cards);  • IASME (Small to Medium sized enterprises);  • NIST (US government and international defence). |
|  | Describe the impact of the General Data Protection  Regulation (GDPR) on the following sectors, and identify what actions should be taken to meet the Regulation:  • Government (both central and local) - including Social and Child Protection Services;  • Financial Services;  • Healthcare;  • Law enforcement. |

Understand the roles of experts in the cyber security industry, how they are recognised, and the work they do.

List and understand the key characteristics of the main specialist roles associated with information security, which are:

• Internal:

o Chief information security officer (CISO);

o Security operations centre (SOC) analyst;

o Penetration tester / ethical hacker;

o Governance, risk and compliance (GRC)

manager;

o Security architect;

o Operational security manager.

• External:

o Vulnerability assessors;

o Penetration testers;

o Auditors: ISO 27001 auditors.

o HMG accreditors.

|  |  |  |
| --- | --- | --- |
|  |  | Describe the purpose of the main professional qualifications  for an information security specialist:  • Certified Information Systems Security Professional  (CISSP);  • Certified Information Security Manager (CISM);  • CESG Certified Practitioner (CCP);  • BCS ISEB Certificate in Information Security  Management Principles (CISMP);  • Certified Information Systems Auditor (CISA);  • Certification and Accreditation Professional (CAP);  • Global Information Assurance Certification (GIAC);  • Lead ISO 27001 Auditor;  • Internal ISO 27001 Auditor;  • CHECK Team Leader. |
| Summarise the typical responsibilities of an information  security team:  • Security operations management:  o Security Operations Centres (SOCs);  o fraud investigation;  o data flow control.  • Governance, risk and compliance (GRC);  o regulation management;  o change approval;  o GRC document management;  o compliance.  • Internal and external audit:  o audit event management;  o logistical support. |

Understand the role and purpose of security intelligence information and how to obtain and use these.

• CERT (Computer Emergency Response Team);

• UK National Cyber Security Centre;

• Publicly available government sources (Open Source

Intelligence provider);

• Professional and academic publications;

• Commercial information;

• 'Gray literature' (working papers, unpublished resources).

|  |  |  |
| --- | --- | --- |
| **Qualification**  **Name** | **Learning Outcomes**  **The learner will….** | **Assessment Criteria**  **The learner can…** |
| BCS Level 4  Certificate in Governance, Organisation, Law, Regulation and Standards  **(continued)** | Demonstrate a clear awareness of the legal  framework surrounding intelligence gathering and the relationship to data protection, human rights and privacy. | Explain how the legislation listed below interacts to support  security, privacy, data protection, monitoring and investigations:  • Data Protection Act / GDPR;  • Human Rights Act;  • Regulation of Investigatory Powers Act. |
| Recognise the key security standards that impact information  security:  • The ISO 27000 series of standards;  • The US National Institute of Standards and  Technology (NIST) standards publications;  • The Information Security Forum (ISF) Standard of  Good Practice (SOGP);  • The National Cyber Security Centre (NCSC)  standards:  o CESG Assisted Products Service;  o Commercial Products Assurance.  • The Payment Card Industry Data Security Standard  (PCI-DSS);  • ISO/IECs 15408, 17025 and 20000. |
| Explain the key concepts and benefits of applying ISO27001 to implement an information security management system. | Explain what an Information Security Management System  (ISMS) is. |
| Explain the key concepts of ISO27001. |

|  |  |  |
| --- | --- | --- |
|  |  | Explain how an organisation obtains certification to ISO/IEC  27001. |
| State the benefits of certification to ISO/IEC 27001. |
| Demonstrate a clear awareness of legal and regulatory obligations for breach notification. | Explain which legislation and/or regulation makes security breach reporting mandatory and the reasons for this:  • The Data Protection Act (DPA);  • The General Data Protection Regulations (GDPR);  • The Privacy and Electronic Communications  Regulations (PECR);  • The Human Rights Act (HRA). |
| List, in relation to the UK Data Protection Act and the GDPR:  • The specific time periods permitted within which information security breaches should be reported.  • The authorities that require notification.  • The means by which notification can be undertaken. |

**5. Assessment**

**5.1 Summary of assessment methods**

The qualification is assessed in controlled exam conditions by a one-hour multiple- choice examination, consisting of 40 questions.

The exams are externally marked.

**5.2 Availability of assessments**

To be able to offer BCS Qualifications, you need to become a BCS Approved

Training Provider.

All staff members who are involved in the management, invigilation and training must be registered with BCS. Suitably qualified individuals may be registered for more

than one role. At least two members of staff must be registered with BCS in one of the roles in order for the Training Provider to retain Training Provider approval.

**5.3 Grading**

The exam has a pass mark of 65%.

**5.4 Externally assessed units**

External tests from BCS come in the form of automated tests. The tests offer instant results to the learner.

**5.5 Specimen assessment materials**

A sample test is available on the BCS Website.

**5.6 Support materials**

BCS provides the following resources specifically for these qualifications:

|  |  |
| --- | --- |
| **Description** | **How to access** |
| Syllabus | Available on website |
| Sample tests | Available on website |

**5.7 Access to Assessment**

BCS seeks to provide equal Access to Assessment for all learners, ensuring that there are no unnecessary barriers to assessment and that any reasonable adjustments for learners preserve the validity, reliability and integrity of the qualification.

We will consider requests from BCS approved Training Providers for reasonable adjustments and special considerations to be approved for a learner. The decision will be based on the individual needs of the learner as assessed by suitably qualified professionals. In promoting this policy, BCS aims to ensure that a learner is not disadvantaged in relation to other learners and their certificate accurately reflects their attainment.

**6. Contact Points**

BCS Qualifications Client Services is committed to providing you with a professional service and support at all times through a single, dedicated point of contact. With a flexible and proactive approach, our team will work together with you to ensure we deliver quality solutions that are right for you.

BCS, The Chartered Institute for IT

First Floor, Block D, North Star House, North Star Avenue, Swindon SN2 1FA

T: +44 (0) 1793 417 424;

W: [www.bcs.org/qualifications](http://www.bcs.org/qualifications)

If you require this document in an accessible format, please call +44 (0) 1793 417 424

© BCS, The Chartered Institute for IT, is the business name of The British Computer

Society (registered charity no. 292786).