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 6.0

August 2020

Contents

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) and Occupational Brief (Click here) 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.	85 (56h + 28h + 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.	94 (62h + 31h + 1h)
5. BCS Level 4 Certificate in Employment of Cryptography.	125 (83h + 41h + 1h)
6. BCS Level 4 Award in Risk Assessment.	119 (79h + 39h +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 what information assets and information processing systems are.
		Explain why information assets and related systems need to be protected.
		Describe the impact, negative or positive, a security incident could have on an organisation. • Financial; • Operational; • Reputational; • Legal; • Regulatory.
		Discuss how information and cyber security impacts different types of organisations. • Public; • Private; • CNI; • Different industries; • Different geographical locations; • Large enterprise; • Small business; • Charity/non-profit.

		Describe how information and cyber security can affect society: • Citizens; • Not for profit groups; • Public services.
	Describe and explain the terminology and basic concepts of cyber security.	Describe confidentiality, integrity, availability, identity, authentication and nonrepudiation.
		Explain how threats and vulnerabilities create risk.
		Explain how likelihood and impact are used to determine risk and how this is recorded. • Risk register.
		Describe how defending information assets and related systems is asymmetric because every risk needs to be treated whilst attackers only need to exploit one.
		Describe sources of threats and their capability, motivations and opportunity. • Individuals; • Groups (criminal and political); • Nation states; • Insiders (deliberate or accidental).
		Describe how environmental hazards and inadequate system design and maintenance create risks.
		Explain how the organisation's culture and security objectives govern the types of controls selected.

		Explain how risk appetite is determined and what risk treatment options are available. • Accept; • Reduce; • Avoid; • Transfer or share.
	Explain security assurance concepts and practices.	Explain what 'trusted' (e.g. proven through the use of PKI certificates) and 'trustworthy' (e.g. implied by the use of secure development methodologies) mean when applied to information security assurance.
		Explain what is meant by the following approaches to assurance and describe when they can be used: • Intrinsic assurance (confidence in the process used by the supplier during development by following a recognised standard); • Extrinsic assurance (independent of the development environment using external evaluation); • Design & implementation (designed and implemented to a recognised standard); • Operational policy & process (operated and maintained to a recognised standard).
		Explain that penetration testing is a form of assurance ideally carried out by professionals using industry recognised ethical methods to test the technical and organisational controls in place. • Pen test; • Red team exercise; • Bug/bounty hunter.

		Describe the benefits and limitations of extrinsic assurance methods. • Security testing (an automated review against known vulnerabilities only); • Supply chain testing (point in time audit of suppliers' technical and organisational controls against a recognised standard of their compliance with legal and regulatory requirements); • Common criteria (a review of the organisations requirements against a standard specific to the technology).
		Describe ways an organisation can use intrinsic assurance. • What certificates does the supplier hold e.g. ISO27001. ISO9001; • What standards have a supplier's products been certified against e.g. FIPS.
	Understand how to apply basic security concepts.	Describe what security objectives and security requirements are and what they should include: • Functional requirements; • Non-functional requirements; • Relative priority (MoSCoW); • KPI's; • Responsibility.

		Justify how security objectives are applied to information assets and infrastructure assets in different business scenarios depending on the value of the asset and the part the asset plays in the scenario. • Migrating from an on-premise solution to a cloud service; • Developing a new product that uses customer data; • Outsourcing key business process.
	Describe security concepts applied to ICT infrastructure.	Describe common vulnerabilities in computer network and systems: • Non-secure coding; • Inadequate traffic filtering; • Missing patches and updates; • Inappropriate configuration; • Insecure protocols; • Lack of malware protection; • Inadequate access controls (identification, authentication, authorisation, ACLs); • Inappropriate design and architecture; • Lack of consideration of environmental factors; • Inadequate physical security controls; • Interoperability.

		Describe the building blocks of computers, networks and the internet: • Input devices; • Output devices; • Routers; • Switches; • Hubs; • Wireless access points and controllers; • Clients and servers; • Local and networked storage; • Network transmission media; • Industrial control systems; • Data centres.
		Describe typical architectures of computers, networks and the internet. • Wireless and wired; • Operating systems; • Fat and thin clients; • Physical and virtual; • Hub and spoke; • Mesh network; • Redundant hardware and transmission paths.

Qualification Name	Learning Outcomes The learner will….	Assessment Criteria The learner can…
BCS Level 4 Certificate in Cyber Security Introduction. **(continued)**	Describe and explain common sources of threat and attack techniques.	Describe the main attack techniques and explain how they work and where are successful: • phishing and its variations; • social engineering; • malware; • network interception; • advanced persistent threats; • DOS and DDOS; • Physical theft; • Business email compromise.
		List insider threats • Malicious employee; • Negligent employee; • Inadequately trained employee; • Unmanaged 3rd party staff.
		Describe the factors that contribute to a negative or positive cyber security environment. • Management direction through policy; • Communication; • Training and awareness; • Incident reporting; • Roles and responsibilities; • Whistleblowing.

		Explain how a threat is the results of an attack technique combined with the motive and opportunity.
		• Motive;
		  ○ Criminal;
		  ○ Political;
		  ○ Reputational.
		• Opportunity;
		  ○ M&A;
		  ○ Fluctuations in currency or asset value;
		  ○ Changes to technology;
		  ○ Change in personnel;
		  ○ Changes in political landscape;
		  ○ New vulnerabilities in products disclosed.

		Describe how environmental hazards such as fire and flood can results in the same impact as an attack.

Qualification Name	Learning Outcomes The learner will….	Assessment Criteria The learner can…
BCS Level 4 Certificate in Cyber Security Introduction. **(continued)**	Describe cyber defence techniques.	List the main defensive techniques, classify them as deter protect, detect or react and describe how they can be used together to create defence in depth. • Perimeter controls; • Traffic filtering; • Least privilege; • Authentication and authorisation; • Anti- malware; • Application whitelisting; • Proactive monitoring; • Secure configuration; • Intrusion detection and prevention; • File integrity monitoring; • Data loss prevention; • Patching and updating; • Change control; • Encrypted connections.

		Describe the benefits of using the MITRE ATT&CK model. • Initial access; • Execution; • Persistence; • Privileged escalation; • Defence evasion; • Credential access; • Discovery; • Lateral movement; • Collection; • Exfiltration; • Command and control.
	Describe and explain legislation, standards, regulations and ethical standards relevant to cyber security.	Describe the cyber security standards and regulations and their consequences for the following sectors: • Government (HMG Security Policy Framework, Cyber Essentials); • Finance (PCI-DSS, NIST, ISO27001, FCA, PRA, CBEST); • Defence (Def Stan 05-138, JSP440, JSP604, NIST) • CNI (NISD, Operational Guidelines for Industrial Automated Control Systems (ICAS).
		Explain the role of laws and regulations on cyber security with reference to: • Criminal law (e.g. Computer Misuse Act, Data Protection Act): • Contract law (service delivery management and meeting SLAs); • Industry specific regulations (e.g. finance, health).

		Explain the benefits, costs and motives for uptake of security standards by organisations including: • PCI-DSS; • ISO27001; • Cyber Essentials.
		Describe the key features of relevant UK law that affect cyber security for individuals and organisations including; • Computer Misuse Act; • Data Protection Act; • Human Rights Act; • Copywrite, Designs and Patents Act.
		Describe the key features of relevant international laws and regulations and their implications for cross border movement of data and products including: • Digital Millennium Act; • ITAR; • EU-US Privacy Shield (replaced Safe Harbour); • General Data Protection Regulation; • Patriot Act.
		Describe the legal responsibilities of systems users and how the following are used to communicate them: • Acceptable use policies; • Logon banners; • Training and awareness programmes.

		Describe the ethics and codes of conduct for cyber security professionals with reference to following professional bodies: • BCS; • CIISec (formally IISP); • ISACA; • (ISC).
	Describe how to keep up with the threat landscape.	Describe horizon scanning with reference to the following source types: • Market trend reports (vendor reports, Gartner, ISF); • Academic research papers; • Professional journals (e.g. IEEE, IET, Oxford Academic, BCS); • Hacker conferences (e.g BlackHat, Bsides); • Government sponsored, online sources (e.g. CiSP, ENISA).
		Describe diversity when using horizon scanning with reference to: • Delphi method; • Trend impact analysis.
	Describe trends on cyber security and explain the value of analysing future trends.	Describe trends in cyber security and their significance. • IoT security; • AI; • Quantum computing.

		Explain the value and risk of analysing future trends. • Future proofing investment in technology; • Including future security requirements when planning changes and upgrades; • Under investing in categories of controls; • Training cyber security professionals in the right skills.

Qualification Name	Learning Outcomes The learner will….	Assessment Criteria The learner can…

BCS Level 4 Certificate in Network and Digital Communications	Explain what is meant by data and protocols and how they relate to each other.	Describe the OSI and TCP/IP models and example protocols.
		• Application:
		  ○ HTTP/S;
		  ○ SNMP;
		  ○ SMTP.
		• Transport;
		  ○ TCP;
		  ○ UDP.
		• Internet:
		  ○ IPv4 and IPv6;
		  ○ ICMP.
		• Link:
		  ○ Ethernet.

		Explain what a network protocol is and how it transmits data with reference to: • Host addressing; • Frames; • Packets; • Datagrams; • Data.

		Describe how protocols can fail and give examples of communication errors at different OSI layers. • Failure to find a route to a host; • Failure to negotiate an encryption method; • Failure to receive or acknowledge packets; • Failure to agree packet formats; • Failure to agree transmission speed or duplex models.
		Describe how error controls is applied to protocols.
		Explain what a routing protocol does and the difference between static and dynamic routing.
		Describe the main routing protocols in current use, describing the pros and cons of each and when they are used: • RIPv2 and RIPng; • OSPF; • BGP; • EIGRP; • IS-IS.
	Explain some of the main factors that affect network performance and propose ways to improve performance.	Explain how network performance can be affected by various factors including: • Available bandwidth; • Number of users; • Applications in use; • WAN connection.

		Describe ways to improve network performance including: • Using QOS; • Traffic shaping and throttling; • Increasing local capacity; • Reducing WAN contention; • Increasing network bandwidth; • Using VLANs; • Restricting application use; • Restricting traffic at the border.

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 what good practice in design is and how this may contribute to security.	Describe the features of good systems design and explain how these contribute to security:
		• OWASP Security by Design Principles:
		  ○ Minimize attack surface area;
		  ○ Establish secure defaults;
		  ○ Principle of least privilege;
		  ○ Principle of defence in depth;
		  ○ Fail securely;
		  ○ Don't trust services;
		  ○ Separation of duties;
		  ○ Avoid security by obscurity;
		  ○ Keep security simple;
		  ○ Fix security issues correctly.

		Describe the facets of software trustworthiness as defined by The Trustworthy Software Framework and explain how each can be explicitly and implicitly assessed against an organisation's security requirements: • Safety; • Reliability; • Availability; • Resilience; • Security.

		Explain the four levels of trustworthiness, how the control sets apply and explain under what circumstances each might be appropriate. • TL1 Essential Practices; • TL2 Assessed Practices; • TL3 Enhanced Practices; • TL4 Specialist Practices.

	Describe common security architectures that incorporate security hardware and software components and be aware of sources of reputable security architectural patterns and guidance.	Explain the purpose and nature of security architecture and how it differs from enterprise architecture considering all the technology, people and processes relating to a computer system.
		• NCSC secure design principles:
		  ○ Establish the context;
		  ○ Making compromise difficult;
		  ○ Making disruption difficult;
		  ○ Making compromise detection easier;
		  ○ Reducing the impact of compromise.

		Explain the common security architecture frameworks in use. • TOGAF; • MODAF; • Zachman; • SABSA; • NIST; • COBIT.

		List reputable sources of architectural patterns and guidance. • NCSC; • NIST; • Vendors.
	Understand how to develop a 'security case', recognising that threats evolve and threats also respond to a security design.	Describe the purpose of a security case.
		List the key characteristics of a security case. • Business contexts; • Security objectives; • Threats and vulnerabilities; • Mitigation options; • Technical controls; • Organisational controls; • Cost benefit considerations; • Legal and regulatory environment; • Implantation activities.
		Describe the resources available to aid with development of a security case and how they can be used. • Common Criteria; • FIPS 140; • NCSC CAPS.

		Describe how threats can be modelled using the STRIDE example. • Spoofing; • Tampering; • Repudiation; • Information disclosure; • Denial of service; • Elevation of privilege.
		Describe how threats change in response to security architecture and how threat modelling may need to change as a result of the outcome.

BCS Level 4 Award in Security Technology Building Blocks	Describe common types of security hardware and software which are used to protect systems, explain how each may be used and understand the benefits and limitations of each.	Describe the main categories of security hardware and software that are available to assist with risk mitigation.
		• Network protection;
		  ○ Network firewalls (perimeter, internal, DMZ);
		  ○ IDS / IPS;
		  ○ Web security / proxy;
		  ○ Email security / MTA;
		  ○ DNS filtering;
		  ○ UTM;
		  ○ Web application firewalls;
		  ○ DLP;
		• Host protection;
		  ○ Antivirus / anti-malware / EDR;
		  ○ HIDS;
		  ○ Software policies and permissions;
		• Proactive monitoring;
		  ○ SIEM;
		  ○ FIM;
		  ○ Network traffic monitoring;
		  ○ Honeypots;
		• Encryption technology;
		  ○ WDE;
		  ○ File encryption;
		  ○ Message / traffic encryption;
		  ○ Database encryption;
		  ○ Removable media encryption;
		  ○ HSM;
		  ○ TPM;

		• Identify and access management;
		  ○ Authentication technologies;
		  ○ Authorisation;
		  ○ Access controls (physical, NAC, ACLs);
		  ○ Enterprise IDM solutions.

		Explain how each security hardware and software category listed helps to protect data and systems explaining what threat or vulnerability they are designed to address.
		Explain how the security hardware and software category listed is employed as part of a defence in depth approach with reference to the stages of the attack chain they are designed to address using the MITRE ATT&CK model. • Initial access; • Execution; • Persistence; • Privileged escalation; • Defence evasion; • Credential access; • Discovery; • Lateral movement; • Collection; • Exfiltration; • Command and control.

		Describe how implicit assurance can be used to help select security hardware and software in different situations. • What security certifications does the supplier hold; • What frameworks or standards do they claim to follow; • What industry specific standards or codes of practice do they adhere to; • What do industry analysts and other customers say about the organisation or products; • What standards have a supplier's products been certified against.
		Describe the limitations of the various security hardware and software categories listed and the common ways in which they can be defeated by skilled and determined adversaries.
		Explain the benefits and risks of selecting open source solutions as part of a security strategy. • Free licence; • Auditable; • Editable / configurable; • Community support; • Lack of SLA for support and maintenance; • May include untrustworthy code.

Qualification Name	Learning Outcomes The learner will….	Assessment Criteria The learner can…

BCS Level 4 Certificate in Employment of Cryptography	Describe main cryptographic techniques and explain the significance of key management and the main features of cryptosystems.	Describe the main cryptographic techniques in use.
		• Symmetric;
		  ○ Stream ciphers (e.g. RC4, ChaCha);
		  ○ Block ciphers (e.g. RC5, AES, 3DES, Blowfish);
		• Asymmetric or public key;
		  ○ RSA;
		  ○ Diffle-Hellman;
		  ○ PGP;
		  ○ Elliptic curve ciphers;
		• Hashing;
		  ○ MD5;
		  ○ SHA.

		Describe how the main cryptographic techniques are used and the limitations of each in those situations.
		• File and disk encryption;
		  ○ Removable media;
		  ○ WDE for storage in desktops and servers;
		  ○ Mobile phones;
		  ○ Individual document encryption;
		• Database encryption;
		  ○ Individual fields or records;
		  ○ Transparent whole database encryption;
		• Digital rights management;
		  ○ Product keys;
		  ○ Copy protection for electronic media;
		  ○ DVD encryption;
		  ○ Online authentication or activation;
		• Ransomware;
		  ○ Removing access to files;
		  ○ Key recovery;
		• Ecommerce;
		  ○ TLS/SSL protected transactions;
		  ○ Cryptocurrency;
		• Wireless communications;
		  ○ WLANs;
		  ○ Wireless WAN backhaul;
		• Email;
		  ○ Message encryption;
		  ○ Message signing;
		• Data destruction;
		  ○ Destroying keys to remove access to data;

		• Blockchain.

		• Protecting passwords and other authentication mechanisms;
		  ○ Hashing passwords;
		  ○ Password managers;
		  ○ Protecting biometrics;
		  ○ Smart cards;
		• VPNs;
		  ○ User authentication;
		  ○ Network to network authentication;
		  ○ Traffic encryption.

		Explain how crypto systems are attacked. • Replay attacks; • Side channel; • Traffic analysis; • Brute force; • MTM; • Key theft.
		Explain how crypto systems and algorithms become obsolete and can be poorly implemented. • DES; • WEP; • MD5; • SHA1.

		Describe the features of key management including the key lifecycle and the challenges associated with each stage. • Generate; • Distribute; • Deploy; • Archive; • Revoke; • Destroy.
		Explain how key management works in symmetric and asymmetric cryptosystems describing the benefits and limitations of each. • Open and closed source key management systems; • Cloud based key management services; • PKI and digital certificates.
		Explain the significance of entropy in cryptography.
	Describe the role of cryptographic techniques in a range of different systems and recognise the legal issues relevant to cryptography.	Describe how cryptographic techniques are used in different systems and the practical difficulties of each in those situations including how to introduce and maintain them in an existing ecosystem. • Cellular radio e.g. GSM and professional radio e.g. TETRA; • Chip and PIN enabled payment cards; • Authentication tokens; • File and desk encryption in desktop operating systems; • Online transactions using TLS/SSL; • 'chat' communications e.g. Whatsapp, iMessage; • Password managers.

		Recognise that there are legal issues surrounding cryptography when crossing national borders or exporting / importing cryptographic technology.
		Describe the purpose of the Wassenaar Arrangement and how it impacts on cryptography.

Qualification Name	Learning Outcomes The learner will….	Assessment Criteria The learner can…
BCS Level 4 Award in Risk Assessment	Describe relevant risk assessment methodologies commonly used in the context of information security and know how to apply them in practice.	Describe how vulnerabilities and threats combined with likelihood and impact create risk and describe potential business consequences of the impact in terms of: • Confidentiality; • Integrity; • Availability; • Productivity; • Financial; • Legal and regulatory; • Health and safety; • Reputation.
		Describe commonly used risk assessment methodologies and their features: • ISF information Risk Assessment Methodology 2 (IRAM2); • ISACA Risk IT; • NIST SP 800-30; • Octave; • Factor Analysis of Information Risk (FAIR).

		Explain how risk methodologies are used in different types of organisations and situations. • Component-driven; • System-driven; • SME's; • Enterprises; • Public Sector; • Military; • CNI.
	Demonstrate an understanding of the differences of threats and vulnerabilities.	Describe the main sources of vulnerabilities and how to identify their relevance in various circumstances: • OWASP Top 10; • Hardware design and implantation; • Software design and development; • Inadequate testing; • Poor configuration and integration; • Poor patch management; • Inadequate network defences; • Lack of encryption or access controls; • Lack of training and awareness; • Poor or missing documentation; • Inherent environmental factors; • Lack of monitoring – lack of auditing; • Poor policy and process; • Weak security culture; • Organisational culture e.g M&A.

		Explain how organisations (management, training, policy and procedure) and technical (physical and logical) security can be linked to create new vulnerabilities or change their severity, including how people can be the weak link or greatest asset.
		Describe what 'cyber culture' in an organisation is and how it can be improved or diminished e.g. • Management commitment; • Accountability; • Employee awareness campaigns; • Employee training; • Rewards and punishments; • Employment contracts; • Policies and procedures; • What incidents occur and how they are managed: • Whistleblowing.

		Describe the main sources of threats and threat actors and how to identify their relevance in various circumstances with reference to:
		• Threat categories and models:
		  ○ Environmental event;
		  ○ Hardware failure;
		  ○ Software failure;
		  ○ Capacity problems;
		  ○ Information theft;
		  ○ Information disclosure;
		  ○ Malware;
		  ○ Phishing;
		  ○ DOS & DDOS;
		  ○ Ransomware and crypto mining;
		  ○ Microsoft STRIDE;
		  ○ CVSS;
		• Threat actors (opportunity, motive, capability):
		  ○ Insiders;
		  ○ Individuals;
		  ○ Political groups;
		  ○ Activists;
		  ○ Organised crime;
		  ○ State sponsored.

		Describe threat intelligence sources and explain the intelligence lifecycle.
		• Sources;
		  ○ Government e.g. NCSC;
		  ○ Commercial feeds;
		  ○ Vulnerability databases;
		  ○ OSINT;
		  ○ Industry forums;
		  ○ In-house expertise and internal systems;
		  ○ Dark web, social media and forums;
		• Lifecycle;
		  ○ Direction;
		  ○ Collection;
		  ○ Processing;
		  ○ Analysis;
		  ○ Dissemination;
		  ○ Feedback.

Qualification Name	Learning Outcomes The learner will….	Assessment Criteria The learner can…

BCS Level 4 Award in Risk Assessment
(Continued)
	Describe different approaches to risk treatment and management.	Describe the steps in risk treatment and explain when the various treatment options might be appropriate in relation to risk appetite with reference to:
		• ISO27005;
		  ○ Reduce;
		  ○ Retain;
		  ○ Avoid;
		  ○ Transfer;
		• NIST SP 800-30;
		  ○ Assumption;
		  ○ Avoidance;
		  ○ Limitation;
		  ○ Planning;
		  ○ Research and acknowledgment;
		  ○ Transference.

		Explain the role of risk owner and how their view of risk may differ from that of other stakeholders who may have other financial or operational priorities.

		Describe the features, benefits and drawbacks of qualitative and quantitative risk measurement methods and when each might be used.
		• Qualitative using:
		  ○ 3x3 or 5x5 grid with likelihood and impact leading to low medium and high risks;
		• Quantitative using:
		  ○ Exposure Factor (EF);
		  ○ Single Loss Expectancy (SLE);
		  ○ Annualised Rate of Occurrence (ARO);
		  ○ Annualised Loss Expectancy (ALE).

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:
		• the Main Board;
		  ○ the Risk Management Committee;
		  ○ the Information Security Management Board.
		• Governance roles:
		  ○ the Main Board;
		  ○ executives;
		  ○ audit;
		  ○ information security;
		• Management planning:
		  ○ strategic direction;
		  ○ objectives setting;
		  ○ risk management;
		  ○ 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;
		  ○ risk;
		  ○ asset;
		  ○ 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.

Qualification Name	Learning Outcomes The learner will….	Assessment Criteria The learner can…

BCS Level 4 Certificate in Governance, Organisation, Law, Regulation and Standards
(Continued)
	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:
		  ○ swipe cards;
		  ○ PINs;
		  ○ biometrics.

Qualification Name	Learning Outcomes The learner will….	Assessment Criteria The learner can…

BCS Level 4 Certificate in Governance, Organisation, Law, Regulation and Standards
(Continued)
	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:
		  ○ management;
		  ○ employees;
		  ○ shareholders;
		  ○ representative bodies;
		• The major forces in the external environment:
		  ○ political;
		  ○ economic;
		  ○ technological;
		  ○ socio-economic;
		  ○ 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.

Qualification Name	Learning Outcomes The learner will….	Assessment Criteria The learner can…

BCS Level 4 Certificate in Governance, Organisation, Law, Regulation and Standards
(Continued)
	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:
		  ○ Chief information security officer (CISO);
		  ○ Security operations centre (SOC) analyst;
		  ○ Penetration tester / ethical hacker;
		  ○ Governance, risk and compliance (GRC) manager;
		  ○ Security architect;
		  ○ Operational security manager.
		• External:
		  ○ Vulnerability assessors;
		  ○ Penetration testers;
		  ○ Auditors: ISO 27001 auditors;
		  ○ 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.
		Explain the main information security roles that tend to be undertaken by, often external specialists: • Vulnerability assessors; • Penetration testers; • Auditors; ○ ISO 27001 auditors; • HMG accreditors.

		Summarise the typical responsibilities of an information security team:
		• Security operations management:
		  ○ Security Operations Centres (SOCs);
		  ○ fraud investigation;
		  ○ data flow control;
		• Governance, risk and compliance (GRC);
		  ○ regulation management;
		  ○ change approval;
		  ○ GRC document management;
		  ○ Compliance;
		• Internal and external audit:
		  ○ audit event management;
		  ○ 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:
		  ○ CESG Assisted Products Service;
		  ○ Commercial Products Assurance;
		• The Payment Card Industry Data Security Standard (PCI-DSS);
		• ISO/IECs 15408, 17021 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 that the General Data Protection Regulations (GDPR), Article 33, makes data breach reporting mandatory to the Information Commissioners Office (ICO). Apprentices must be able to explain the impact of a breach in security and the unauthorised release of personal data with relation to the following legislation: • The Privacy and Electronic Communications Regulations (PECR); • The Human Rights Act (HRA); • Data Protection Act (DPA).
		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%.

Please note: Whilst BCS would not normally want to make changes to either grade thresholds or grading algorithms there is potential for them to change in order to maintain standards.

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

3 Newbridge Square

Swindon

SN1 1BY

T: +44 (0) 1793 417 424;

W: www.bcs.org/qualifications

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