Making IT good for society

Qualification Specification for the Knowledge Modules that form part of the BCS Level 4 Cyber Intrusion Analyst Apprenticeship

BCS Level 4 Award in Network
BCS Level 4 Award in Operating Systems
BCS Level 4 Certificate in Information and Cyber Security Foundations
BCS Level 4 Award in Business Processes
BCS Level 4 Award in Law, Regulation and Ethics

Version 3.2
February 2019

Making IT good for society

BCS Level 4 Cyber Intrusion Analyst Qualification Specification

Contents

Change History

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

Version Number	Changes Made
V1.0	Document created.
V2.0	Change to exemptions text.
V3.0	Modules 3, 4 and 5 added.
V3.1	Edit to learning outcome on page 29 to reflect change in Law, Regulation and Ethics Syllabus.
V3.2	External links updated.

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, information the design of 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. 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
BCS Level 4 Award in Network	**603/2892/7**	**26/01/2018**
BCS Level 4 Award in Operating Systems	**603/2894/0**	**26/01/2018**
BCS Level 4 Certificate in Information and Cyber Security Foundations	**603/3214/1**	**01/06/2018**
BCS Level 4 Award in Business Processes	**603/3215/3**	**01/06/2018**
BCS Level 4 Award in Law, Regulation and Ethics	**603/3216/5**	**01/06/2018**

The five knowledge module qualifications listed above have been developed based on the requirements set out in the Standard issued by 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.

An apprentice needs to have passed the five knowledge module qualifications (mentioned in the above table) before being able to move on to the End Point Assessment to complete their apprenticeship.

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 Intrusion Analyst 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 Intrusion Analyst is to detect breaches in network security for escalation to incident response or other determined function. An Intrusion Analyst will typically use a range of automated tools to monitor networks in real time, will understand and interpret the alerts that are automatically generated by those tools, including integrating and correlating information from a variety of sources and in different forms and where necessary seek additional information to inform the Analyst's judgement on whether or not the alert represents a security breach. When an Analyst has decided that a security breach has been detected, he or she will escalate to an incident response team, or other determined action, providing both notification of the breach and evidence with reasoning that supports the judgement that a breach has occurred. An Analyst will typically work as part of a team (or may lead a team) and will interact with external stakeholders, including customers and third-party sources of threat and vulnerability intelligence and advice

3.3 Structure of the qualifications

This document covers the following qualifications which are used towards the Level 4 Cyber Intrusion Analyst Apprenticeship. The qualifications can be taken in any order however it is recommended that they be completed in the following sequence:

1. BCS Level 4 Award in Network
2. BCS Level 4 Award in Operating Systems
3. BCS Level 4 Certificate in Information and Cyber Security Foundations
4. BCS Level 4 Award in Business Processes
5. BCS Level 4 Award in Law, Regulation and Ethics

Qualification Level 4 Descriptor	
Knowledge descriptor (the holder…)	The apprentice will understand IT network features and functions, including virtual networking, principles and common practice in network security and the OSI

	and TCP/IP models, and the function and features of the main network appliances. They can utilise at least three Operating System (OS) security functions and associated features. The apprentice will understand and be able to apply the foundations of information and cyber security including: explaining the importance of cyber security and basic concepts including harm, identity, confidentiality, integrity, availability, threat, risk and hazard, trust and assurance and the 'insider threat' as well as explaining how the concepts relate to each other and the significance of risk to a business. They understand and are able to propose appropriate responses to current and new attack techniques, hazards and vulnerabilities relevant to the network and business environment. They can also understand and propose how to deal with emerging attack techniques, hazards and vulnerabilities relevant to the network and business environment. They will understand lifecycle and service management practices to Information Technology Infrastructure Library (ITIL) foundation level. Candidates will understand and can advise others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation. They will understand the main features and applicability of law, regulations and standards (including Data Protection Act/Directive, Computer Misuse Act, ISO 27001) relevant to cyber network defence and follows these appropriately. The apprentice will understand, adhere to and advise on the ethical responsibilities of a cyber security professional.
Skills descriptor (the holder should have…)	Apprentices will develop skills and be able to demonstrate; logical and creative thinking skills; analytical and problem-solving skills, ability to work independently and take responsibility; can use own initiative; a thorough and organized approach, ability to work with a range of people; ability to communicate effectively in a variety of situations; maintain productive, professional and secure working environment

3.4 Prior learning

The only pre-requisite to take the qualifications is enrolment on the Level 4 Cyber Intrusion Analyst Digital IT Apprenticeship.

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 Intrusion 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 assess 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)**
BCS Level 4 Award in Network	119h (68h + 50h + 1h)

BCS Level 4 Award in Operating Systems	69h (38h + 30h + 1h)
BCS Level 4 Certificate in Information and Cyber Security Foundations	233h (97.5h + 134h + 1h)
BCS Level 4 Award in Business Processes	81h (53h + 26.5h + 1h)
BCS Level 4 Award in Law, Regulation and Ethics	80h (53h + 26.5h +0.5h)

4.2 Learning outcomes and assessment criteria

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
BCS Level 4 Award in Network	Describe and explain the common networks in use and their associated data formats and protocols.	Describe the components and equipment of a network. • hubs; • switches (L2 and L3); • bridges; • WAPs; • routers; • firewalls; • proxy servers.
		Explain the features of network protocols in widespread use on the Internet. • HTTPS; • HTTP; • SMTP; • SNMP; • TCP; • UDP; • IP.
		Summarise the main security controls and appliances employed in digital networks.

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

	Be able to explain network layer models and then identify their differences.	Identify all seven layers and representative protocols at each layer within the OSI model.
		• the Physical layer;
		  ○ electrical;
		  ○ optical;
		  ○ wireless.
		• the Data Link layer;
		  ○ purpose of the Data Link layer;
		  ○ data format;
		  ○ description of an Ethernet frame;
		• the Network layer;
		  ○ purpose of the Network layer;
		  ○ Internet Protocol;
		• the Transport layer;
		  ○ purpose of the Transport layer;
		  ○ Transport layer protocols (TCP and UDP);
		• the Session layer;
		  ○ purpose of the Session layer;
		• the Presentation layer;
		  ○ purpose of the Presentation layer;
		• the Application layer;
		  ○ purpose of the Application layer.

		Summarise the differences between the following Physical layer categories and Data Link layer protocols: • Physical layer - wireless, fibre, wired; • Data Link layer - Ethernet [802.3], wireless LAN [802.11], Bluetooth and cellular.

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
		Describe the typical approaches and components to implementing VoIP. • terminal (user interface); • gateway; • gatekeeper; • multipoint control unit (MCU).
	Describe and explain network routing protocols.	Describe current network routing protocols in facilitating interoperability in network communications. • RIPv1; • RIPv2; • RIPng; • OSPF; • OSPFv2; • OSPFv3; • EIGRP; • EIGRP for IPv6.
		Describe the differences between LAN and WAN scenarios.
	Understand how network performance can be affected.	Identify the factors that affect network performance. • bandwidth; • number of users; • contention.
	Describe and explain the factors that affect network performance.	Summarise the key features of IEEE 802 standards. • local area networks (LANs); • metropolitan area networks (MANs).

	Learn the principles of network addresses.	Explain and demonstrate the purpose and features of IP.
		• IP addressing - definition of network and host addresses;
		• classful addressing (class A, B, C, D, E);
		  ○ IP address allocation;
		  ○ IP address format
		  ▪ binary;
		  ▪ dotted decimal notation;
		  ○ network and broadcast addresses;
		• IP header format;
		  ○ type of service (TOS) field;
		  ○ protocol field;
		  ○ time to live (TTL) field;
		  ○ checksum;
		• IP scaling problems;
		  ○ growth of Internet;
		  ○ subnet masks – the need for 3rd level of hierarchy;
		  ▪ subnet mask format;
		  ▪ logical AND operation;
		  ▪ public and private addresses;
		  ▪ default gateway;
		  ○ static and dynamic address allocation;
		  ▪ Dynamic Host Configuration Protocol (DHCP);
		  ▪ DHCP server requirements;
		  ▪ the DHCP process (DORA);
		  ▪ DHCP lease;
		  ▪ domain names;
		  ▪ domain name resolution;
		  ▪ requirements of DNS servers;
		  ▪ host name resolution (7 step sequence);
		  ▪ NetBIOS name resolution (6 step sequence);
		  ▪ subnetting (and supernetting) networks;
		  ▪ design considerations (the 4 key questions);
		• purpose of IP v6;
		  ○ benefits of IP v6;

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
		○ extended address space.
BCS Level 4 Award in Operating Systems	Describe and explain the common configurations of operating system's (OS) firewalls.	Explain how to configure an OS firewall. • OS Linux; • IOS; • Windows.
		Explain the rational for configuring an OS firewall. • OS Linux; • IOS; • Windows.
		Describe how to enable / disable OS services for security reasons. • OS Linux; • IOS; • Windows.
		Explain the rationale for enabling / disabling OS services for security reasons. • OS Linux; • IOS; • Windows.
	Explain the differences between user and file access control lists and how to configure them.	Describe how to configure user / file access control list. • Active Directory; • Group Policy; • Share Permissions; • local NTFS files and folders; • registry; • printers.
		Explain how to add and remove domain users and groups.
		Explain the rationale for adding and removing domain users and groups.

	Explain the security features of OS, servers and clients.	Compare and contrast the security features in the following operating systems:
		• Linux;
		  ○ user accounts;
		  ○ file and directory permissions;
		  ○ data verification;
		  ○ secure remote access with OpenSSH;
		  ○ system recovery;
		  ○ resource allocation controls;
		  ○ monitoring and audit facilities;
		  ○ firewall;
		  ○ NFS;
		• Windows;
		  ○ Windows Defender;
		  ○ Device Guard;
		  ○ Windows Hello;
		  ○ Secure Boot;
		  ○ Widows Passport;
		  ○ firewall;
		  ○ Network Access Policy (NAP);
		  ○ DirectAccess;
		  ○ App Locker;
		  ○ Data Execution Prevention (DEP);
		  ○ address space layout randomisation (ASLR);
		  ○ Structured Exception Handler Overwrite Protection (SEHOP);
		  ○ User Account Control (UAC);
		  ○ DNS Security Extensions (DNSSEC);
		• iOS;
		  ○ system security;
		  ○ network security;

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
		○ encryption and data protection; ○ internet services; ○ privacy controls.
		Describe the security features implemented in a server and client. • server; ○ password authentication; ○ firewalls; ○ auditing and accounting; ○ resource sharing; ○ public key infrastructure and SSL / TLS encryption; • client; ○ protection; ○ control; ○ reporting.
	Show an understanding of the need for OS security policies and how to implement a patching policy.	Describe how to implement a patching policy. • detect; • assess; • acquire; • test; • deploy; • maintain.
		Explain the rational and describe how to configure OS security policies for the following: • audit policy settings; • remote desktop service; • system services; • patch management settings; • firewall.

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
BCS Level 4 Certificate in Information and Cyber Security Foundations	Understand basic cyber security concepts and their importance to organisations.	Describe why cyber security is important to organisations. • large corporations; • SMEs.

		Explain how the basic concepts of cyber security can relate to each other.
		• identity;
		• availability;
		• integrity;
		• confidentiality;
		• assurance;
		• threat;
		  ○ external;
		  ○ internal;
		• risk;
		• hazard;
		• harm.

	Understand risk assessment, management and investigation.	Explain how risk assessment and management can benefit an organisation.
		Understand the common terminology, controls and approaches used in risk assessment and management. • vulnerabilities and exploitabilities; • controls.

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
		Understand the types of risks, threats and vulnerabilities, and how they can impact an organisation. • spoofing of user identity; • tampering; • repudiation; • information disclosure (privacy breach or data leak); • Denial of Service (DoS); • elevation of privilege.

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

		Describe the main stages and principles of risk assessment, control and management.
		• components of risk;
		  ○ threat;
		  ○ likelihood;
		  ○ impact;
		• five step composite risk management process;
		  ○ identify hazards;
		  ○ assess hazards to determine risks;
		  ○ develop control measures that eliminate the hazard or reduce its risk;
		  ○ implement controls that eliminate the hazards or reduce their risks;
		  ○ evaluate the effectiveness of controls and adjust / update as necessary;
		• threat modelling;
		  ○ STRIDE (Microsoft);
		  ▪ Spoofing of user identity;
		  ▪ Tampering;
		  ▪ Repudiation;
		  ▪ Information disclosure (privacy breach or data leak);
		  ▪ Denial of Service (DoS);
		  ▪ Elevation of privilege;
		  ○ P.A.S.T.A. (Process for Attack Simulation and Threat Analysis);
		  ○ Trike (a risk-based approach with distinct implementation, threat, and risk models);
		  ○ VAST (Visual, Agile, and Simple Threat modelling);
		• impact levels.

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
		Identify sources of information about threats and vulnerabilities from relevant industry sources. • critical vendors; • governmental and public sources; • private sources.
		Explain how poor security management can adversely impact an organisation.
		Describe the common causes of security incidents. • weak and stolen credentials; • back doors, application vulnerabilities; • malware; • social engineering; • inappropriate permissions granted; • insider threats; • physical attacks; • improper configuration.
		Identify security controls that relate to: • people; • process; • technology.
		Describe the different types of tests that can be used to prepare an organisation. • security auditing; • vulnerability testing; • penetration testing.
		Describe security processes and procedures used within own organisation to maintain operational security.
	Describe and explain all aspects of information governance including policy, legal and regulatory environment, information assurance, information security awareness and audit.	Explain the term information governance and the potential impacts of poor information governance.
		Recognise the need for information security policy to achieve information security.

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
		Describe what an information security management system (ISMS) is and the potential benefits.

		Describe and explain the following aspects of providing information assurance:
		• methodologies;
		  ○ ISO/IEC 27001;
		  ○ ISO/IEC 27005;
		• processes;
		  ○ staff awareness raising / training;
		  ○ backups;
		  ○ configuration hardening;
		• standards;
		  ○ ISO/IEC 27002;
		  ○ COBIT.

		Describe and explain information assurance methodologies.
		• ISO/IEC 27000 series;
		  ○ ISO/IEC 27001;
		  ○ ISO/IEC 27002;
		• Risk IT;
		• COBIT.

		Identify industry standards bodies and services and provide examples of the services that they provide.
		• BSI (British Standards Institute);
		  ○ product certification;
		  ○ personal training and certification;
		• IAAC (Information Assurance Advisory Council);
		  ○ development of policy recommendations to government and corporate leaders;
		  ○ free workshops.

		Explain how security awareness and training provides benefits to the maintenance of information security.

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

		Describe a variety of methods for improving security awareness.
		• mandatory cyber awareness training;
		• management leading by example;
		• interactive materials;
		  ○ gamification;
		  ○ video;
		• multi vector approach;
		  ○ posters;
		  ○ blogs;
		  ○ e-mail tips;
		  ○ newsletters.

		Identify examples of information security risks caused by poor security awareness. • principle of least privilege (POLP) not implemented; • poor password discipline; • account sharing; • accessing of unsafe internet locations; • installation of non-approved software.
		Explain how audits and reviews contribute to effective security management.
		Identify common sources of information, standards, legislation and accreditation boards that are used to drive and control audit and review processes and practitioners. • BSI (British Standards Institute); • IAAC (Information Assurance Advisory Council); • ISACA (Information Systems Audit and Control Association); • ISSA (Information Systems Security Association (international)); • BCS (British Computer Society).
		Outline the governance controls used within your own organisation.
		Describe local processes for consultation, review and approval.
		Describe audit and review controls used within own organisation.

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
	Demonstrate an awareness of security architecture.	Describe the concept of information security architecture and how it can be used to reduce information risk.
		Explain how information security architecture interacts with other enterprise architectures.
		Describe how security architecture relates to business needs. • Does the nature of the business lead to specific security vulnerabilities? o e-commerce; o child related (schools or colleges); o confidential data related (medical, defence or judicial); o social media; • Does the security architecture provide obstacles to the main business activities? • Will the current security architecture support future developments of the business?
		Understands design patterns or architecture relevant to own work.
	Describe and explain business continuity management approaches, benefits and its relationship with incident management.	Explain the benefits of business continuity management (BCM) and the consequences of poor BCM.
		Explain the relationship of BCM with incident management.
		Describe the steps within the BCM lifecycle and the approaches that can be used to provide business continuity. • ISO 22301; o impact analysis - BIA and TRA; o solution design; o implementation; o testing and organisational acceptance; o maintenance.

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
	Understand how to recognise and respond to an attack.	Describe the possible indicators (signatures) of compromise. • virus signatures; • MD5 hashes or IP addresses of known malware; • known domains or URLs of botnets; • unusual outbound network traffic; • unusual privilege account use; • DNS request anomalies; • web traffic with unhuman behaviour; • signs of DDoS activity.
		Describe the difference between targeted and general and systemic attacks.
		Describe the response options that are available and the main features to implement each. • containment; • eradication; • exploitation; • legal.
		Describe how to scope a response given the objectives for the system under threat.

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

		Describe the process and the benefits of timeline analysis.
		• data sources;
		  ○ audits;
		  ○ event logs;
		  ○ file change timestamps and metadata;
		  ▪ MTF (Windows);
		  ▪ Inode (Linux);
		  ○ tools;
		  ▪ Log2timeline;
		  ▪ packet sniffers;
		  ▪ Plaso;
		  ▪ TimeFlow;
		• benefits;
		  ○ timeline presents complex data in a more human friendly accessible format.

		Prepare action plans based on previous intrusions to reduce the risk of future attacks.

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

	Understand the current cyber security threat landscape and recognise emergent attacks.	Identify the current cyber security threat landscape.
		• known attack techniques;
		  ○ cross-site scripting (XSS);
		  ○ Denial of Service attacks;
		  ○ malware attacks;
		  ○ an-in-the-middle (MITM) attacks;
		  ○ phishing attacks;
		  ○ SQL injection attacks (SQLi);
		• hazards;
		  ○ IoT (increased vulnerability surface);
		  ○ ransomware;
		• vulnerabilities;
		  ○ buffer overflow;
		  ○ lack of encryption;
		  ○ lack of patch management;
		  ○ poor staff security awareness;
		  ○ weak passwords.

		Recognise emergent attack techniques, hazards or vulnerabilities.
		• be aware that it is a constantly changing threat environment;
		  ○ monitor information sources;
		  ▪ news feeds and alerts;
		  ▪ academic research;
		  ▪ hacker forums;
		  ○ evaluate potential emergent attacks against known techniques.

		Describe what assets are affected by an emerging threat and the impact to an organisation. • data; • hardware; • software; • configuration settings; • staff; • buildings and infrastructure.

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
		Describe how a signature or correlation rule is developed in response to the following attack techniques: • intrusion events; • malware events; • abnormal user activity; • traffic profile changes.
		Demonstrate how to write a signature or correlation rule.
BCS Level 4 Award in Business Processes	Describe and explain the lifecycle and service management practices to Information Technology Infrastructure Library (ITIL).	Describe the processes and roles within ITIL that are applicable to a cyber intrusion analyst and describe how they fit into their working practices and environment. • service strategy; • service design; • service transition; • service operation; • continuous service development.
	Describe and explain the different processes for cyber incident response and incident management, as well as how to evidence collection / preservation requirements to support incident investigation.	Describe what a cyber incident response is, its purpose and how it fits into the corporate or business environment. • what the incidence response policies and processes are that are relevant to the cyber intrusion analyst's working environment and role; o Police and Criminal evidence act 1984 (PACE); o GDPR; o Computer Misuse Act 1990; o Regulation of Investigatory Powers 2000 (RIPA). • who to interface with during an incident response process and who to contact; o people; o process; o technology; o information.

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

		Describe the cyber incident management processes.
		• preparation of an organisation;
		  ○ criticality assessment;
		  ○ complete a cyber security threat analysis;
		  ○ consider the implications of people, process, technology and information;
		  ○ create an appropriate control framework;
		  ○ testing the state of readiness;
		• response;
		  ○ identification of security incident;
		  ○ defining objectives and investigate the incident;
		  ○ take appropriate action;
		  ○ recovery of systems, data and connectivity;
		• follow-up activities;
		  ○ complete a thorough investigation of the incident;
		  ○ report the incident and findings to relevant stakeholders;
		  ○ complete and record a post incident review;
		  ○ communicate lessons learnt;
		  ○ update key information, controls and processes;
		  ○ complete a trend analysis.

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

		Explain how the procedure for the collection / preservation of evidence is required to support incident investigation.
		• how to collect and handle data to be provided to an investigation;
		  ○ admissibility of evidence – whether or not the evidence can be used;
		  ○ weight of evidence – the quality and completeness of evidence;
		• how to meet requirements for evidence preservation in accordance with policies and processes relevant to the cyber intrusion analyst's working environment and role;
		  ○ compliance with Association of Chief Police Officers Guidelines on Computer Evidence (ACPO), and the National Police Chiefs' Council;
		  ○ maintain an action log that should include:
		  ▪ identifying information (location, serial number, model number, hostname, Media Access Control addresses, and IP addresses of a hardware);
		  ▪ title, name and contact details of every individual involved in collecting or handling the evidence during the investigation;
		  ▪ date and time of each handling occurrence;
		  ▪ locations where the evidence was stored.

BCS Level 4 Award in Law, Regulation and Ethics	Describe and explain the main features and applicability of law, regulations and standards relevant to cyber network defence.	Describe and explain the relevance of the laws, regulations and standards relevant to the cyber intrusion analyst role. • GDPR; • Computer Misuse Act; • ISO 27001; • Police and Criminal evidence act 1984 (PACE).

Qualification Name	Learning outcomes The learner will….	Assessment Criteria The learner can…
		Describe and explain the relevance of the main regulatory bodies for their industry sector. • 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).
		Identify when to seek authoritative advice and who to contact.
	Describe and explain the ethical responsibilities of a cyber security professional.	Describe the industry recognised code of ethics relevant to cyber security. • SANS Institute; • ISSA (Information Systems Security Association); • The IISP qualification; • CREST; • ISACA's CISM qualification; • ISC2's CISSP qualification; • CCP and CISMP qualifications.
		Describe where ethical behaviour of a cyber-security professional may differ from accepted norms in society. • data integrity / file access; • privacy; • access of personal data and colleague's emails; • key logging / snooping.

5 Assessment

5.1 Summary of assessment methods

The qualification is assessed in controlled exam conditions.

The following modules are assessed using a one-hour multiple-choice examination consisting of 40 questions:

- BCS Level 4 Award in Network
- BCS Level 4 Award in Operating Systems
- BCS Level 4 Certificate in Information and Cyber Security Foundations
- BCS Level 4 Award in Business Processes

The following module is assessed using a 30-minute multiple-choice examination consisting of 20 questions:

- BCS Level 4 Award in Law, Regulation and Ethics

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 exams have 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 specimen 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 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 417 417
E: centresupport@bcs.uk
W: www.bcs.org/qualifications

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