BCS Level 4 Certificate in Cyber Security Introduction Syllabus QAN 603/0830/8

Version 3.0
February 2020

This is a United Kingdom government regulated qualification which is administered and approved by one or more of the following: Ofqual, Qualification in Wales, CCEA or SQA

BCS Level 4 Certificate in Cyber Security Introduction Syllabus

Contents

Change History

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

Version Number	Changes Made
Version 1.0 Nov 2016	Syllabus Created
Version 1.1 Nov 2016	Amended terminology for Harbour
Version 1.2 Nov 2016	Added mandatory Ofqual text
Version 2.0 September 2019	Update to Question Weighting. Removed “including, but not limited to” from all learning outcomes.
Version 3.0 February 2020	Full syllabus review.

Introduction

This certificate is the core module that is applicable to both pathways of the Level 4 Cyber Security Technologist Apprenticeship. This is a general introduction to cyber security and is the core element of the apprenticeship. It covers the essential knowledge foundation for most cyber security roles.

Objectives

Apprentices should be able to demonstrate an understanding of the foundations of cyber security. Key areas are:

1. Explain why cyber security matters.
2. Explain basic security theory.
3. Describe and explain security assurance.
4. Apply basic security concepts to develop security requirements (to help build a security case).
5. Describe security concepts applied to ICT ('cyber') infrastructure.
6. Describe and explain attack techniques.
7. Describe cyber defence.
8. Describe and explain legislation, standards, regulations and ethical standards relevant to cyber security.
9. Understands how to keep up with the threat landscape.
10. Describe future trends.

Evidence of lessons learnt in these key areas should be collected and reflected upon when the Apprentice is compiling the Summative Portfolio as the apprentice could identify how the task might be done better/differently with knowledge subsequently gained.

Target Audience

The certificate is relevant to anyone requiring an understanding of the core principles and foundations of a Cyber Security Technologist.

Course Format and Duration

Apprentices can study for this certificate by attending a training course provided by a BCS accredited Training Provider. The estimated total qualification time for this certificate is 199 hours.

Eligibility for the Examination

There are no specific pre-requisites for entry to the examination; however, apprentices should possess the appropriate level of knowledge to fulfil the objective shown above. Individual employers will set the selection criteria, but this is likely to include A' Levels, a relevant Level 3 apprenticeship, or other relevant qualifications, relevant experience and/or an aptitude test with a focus on functional maths.

Duration and Format of the Examination

The format for the examination is a one-hour multiple-choice examination consisting of 40 questions. The examination is closed book (no materials can be taken into the examination room). The pass mark is 26/40 (65%).

Additional Time for Apprentices Requiring Reasonable Adjustments Due to a Disability

Apprentices may request additional time if they require reasonable adjustments. Please refer to the reasonable adjustments policy for detailed information on how and when to apply.

Additional Time for Apprentices Whose Language Is Not the Language of the Exam

If the examination is taken in a language that is not the apprentice's native/official language, then they are entitled to 25% extra time.

If the examination is taken in a language that is not the apprentice's native/official language, then they are entitled to use their own **paper** language dictionary (whose purpose is translation between the examination language and another national language) during the examination. Electronic versions of dictionaries will **not** be allowed into the examination room.

Guidelines for Accredited Training Organisations

Each major subject heading in this syllabus is assigned an allocated time. The purpose of this is two-fold: firstly, to give both guidance on the relative proportion of time to be allocated to each section of an accredited course and an approximate minimum time for the teaching of each section; secondly, to guide the proportion of questions in the exam. Accredited Training Organisations may spend more time than is indicated and apprentices may spend more time again in reading and research. Courses do not have to follow the same order as the syllabus. Courses may be run as a single module or broken down into two or three smaller modules.

This syllabus is structured into sections relating to major subject headings and numbered with a single digit section number. Each section is allocated a minimum contact time for presentation. Apprentices should be encouraged to consider their Summative Portfolio throughout the modules.

Syllabus

For each top-level area of the syllabus, a percentage and K level is identified. The percentage is the exam coverage of that area, and the K level identifies the maximum level of knowledge that may be examined for that area.

1. Why Cyber Security Matters (12.5%, K2)

In this key topic, the apprentice will describe and explain why information and cyber security are important to businesses and to society. Outcomes should include an ability to:

1.1 Describe what information assets and information processing systems are.

1.2 Explain why information assets and related systems need to be protected.

1.3 Describe the impact, negative or positive, a security incident could have on an organisation.

- financial;
- operational;
- reputational;
- legal;
- regulatory.

1.4 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.

1.5 Describe how information and cyber security can affect society:

- citizens;
- not for profit groups;
- public services.

2. Basic Security Theory (20%, K2)

In this key topic, the apprentice will describe and explain the terminology and basic concepts of cyber security. Outcomes should include an ability to:

2.1 Describe confidentiality, integrity, availability, identity, authentication and nonrepudiation.

2.2 Explain how threats and vulnerabilities create risk.

2.3 Explain how likelihood and impact are used to determine risk and how this is recorded.
- risk register.

2.4 Describe how defending information assets and related systems is asymmetric because every risk needs to be treated whilst attackers only need to exploit one.

2.5 Describe sources of threats and their capability, motivations and opportunity.
- individuals;
- groups (criminal and political);
- nation states;
- insiders (deliberate or accidental).

2.6 Describe how environmental hazards and inadequate system design and maintenance create risks.

2.7 Explain how the organisation's culture and security objectives govern the types of controls selected.

2.8 Explain how risk appetite is determined and what risk treatment options are available.
- accept;
- reduce;
- avoid;
- transfer or share.

3. Security Assurance (12.5%, K2)

In this key topic, the apprentice will explain security assurance concepts and practices. Outcomes should include an ability to:

3.1 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.

3.2 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).

3.3 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.

3.4 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 or their compliance with legal and regulatory requirements);
- Common Criteria (a review of the organisations requirements against a standard specific to the technology).

3.5 Describe ways an organisation can use intrinsic assurance:

- what certifications does the supplier hold e.g. ISO27001, ISO9001;
- what standards have a supplier's products been certified against e.g. FIPS.

4. Applying basic security concepts (5%, K3)

In this key topic, the apprentice understand how to apply basic security concepts. Outcomes should include an ability to:

4.1 Describe what security objectives and security requirements are and what they should include:
- Functional requirements;
- Non-functional requirements;
- Relative priority (MoSCoW);
- KPIs;
- Responsibility.

4.2 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.

5. Security concepts applied to ICT ('cyber') infrastructure (7.5%, K1)

In this key topic, the apprentice will describe security concepts applied to ICT infrastructure. Outcomes should include an ability to:

5.1 Describe common vulnerabilities in computer networks 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

5.2 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.

5.3 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.

6. Attack Techniques and Common Sources of Threat (12.5%, K2)

In this key topic, the apprentice will describe and explain common sources of threat and attack techniques. Outcomes should include an ability to:

6.1 Describe the main attack techniques and explain how they work and where they are successful:

- phishing and its variations;
- social engineering;
- malware;
- network interception;
- advanced persistent threats;
- DOS and DDOS;
- credential theft;
- physical theft;
- business email compromise.

6.2 List insider threats

- malicious employee;
- negligent employee;
- inadequately trained employee;
- unmanaged 3rd party staff.

6.3 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.

6.4 Explain how a threat is the result of an attack technique combined with 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.

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

7. Cyber Defence (5%, K2)

In this key topic, the apprentice will describe cyber defence techniques. Outcomes should include an ability to:

7.1 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.

7.2 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.

8. Legal, Standards, Regulations and Ethical Standards Relevant to Cyber Security (17.5%, K2)

In this key topic, the apprentice will describe and explain legislation, standards, regulations and ethical standards relevant to cyber security. Outcomes should include an ability to:

8.1 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 (IACS)).

8.2 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).

8.3 Explain the benefits, costs and motives for uptake of security standards by organisations including:
- PCI-DSS;
- ISO27001;
- Cyber Essentials.

8.4 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.

8.5 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.

8.6 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.

8.7 Describe the ethics and codes of conduct for cyber security professionals with reference to following professional bodies:
- BCS;
- CIISec (formally IISP);
- ISACA;
- (ISC)^2.

9. Keeping Up with the Threat Landscape (2.5%, K2)

In this key topic, the apprentice will describe how to keep up with the threat landscape. Outcomes should include an ability to:

9.1 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).

9.2 Describe diversity when using horizon scanning with reference to:
- Delphi method;
- trend impact analysis.

10. Trends in Cyber Security (5%, K2)

In this key topic, the apprentice will describe trends on cyber security and explain the value of analysing future trends. Outcomes should include an ability to:

10.1 Describe trends in cyber security and their significance.
- IoT security;
- AI;
- quantum computing.

10.2 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.

Levels of Knowledge / SFIA Levels

This course will provide apprentices with the levels of difficulty / knowledge skill highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated. The levels of knowledge and SFIA levels are explained in on the website www.bcs.org/levels. The levels of knowledge above will enable apprentices to develop the following levels of skill to be able to operate at the following levels of responsibility (as defined within the SFIA framework) within their workplace:

Level	Levels of Knowledge	Levels of Skill and Responsibility (SFIA)
K7		Set strategy, inspire and mobilise
K6	Evaluate	Initiate and influence
K5	Synthesise	Ensure and advise
K4	Analyse	Enable
K3	Apply	Apply
K2	Understand	Assist
K1	Remember	Follow

Question Weighting

Syllabus Area	Target number of questions
1. Why Cyber Security Matters	5
2. Basic Security Theory	8
3. Security Assurance.	5
4. Applying basic security concepts	2
5. Security concepts applied to ICT ('cyber') infrastructure	3
6. Attack Techniques and Common Sources of Threat	5
7. Cyber Defence.	2
8. Legal, standards, regulations and ethical standards relevant to cyber security	7
9. Keeping up with the threat landscape	1
10. Trends in Cyber Security	2
Total	**40 Questions**

Format of Examination

Type	40 Question Multiple Choice.
Duration	1 Hour. An additional 15 minutes will be allowed for apprentices sitting the examination in a language that is not their native /mother tongue.
Pre-requisites	Accredited training is strongly recommended but is not a pre-requisite.
Supervised	Yes.
Open Book	No.
Pass Mark	26/40 (65%).
Calculators	Calculators cannot be used during this examination.
Total Qualification Time (TQT)	199 Hours.
Delivery	Online.

Trainer Criteria

Criteria	▪ Have 10 days' training experience or have a Train the Trainer qualification ▪ Have a minimum of 3 years' practical experience in the subject area

Classroom Size

Trainer to apprentice ratio	1:16

Recommended Reading List

Title: Information Security Management Principles
Author: Taylor, A. *et al.*
Publisher: BCS, The Chartered Institute for IT; 3rd edition
Publication Date: 31 Jan 2020
ISBN-13: 9781780175188

Title: Cyber Security A practitioner's guide
Author: Sutton, D.
Publisher: BCS, The Chartered Institute for IT
Publication Date: 10 Jul 2017
ISBN-13: 9781780173405