BCS Level 4 Certificate in Security Technology Building Blocks Syllabus QAN 603/0884/9

Version 1.1
November 2016

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 Security Technology Building Blocks 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 November 2016	Syllabus Created
Version 1.1 November 2016	Added mandatory Ofqual text

Introduction

This Certificate is the fourth of seven knowledge modules that are applicable to the Technologist learning pathway for the Level 4 Cyber Security Technologist Apprenticeship. This is a general introduction to modern computer networks and it covers the essential building blocks of Security Technology.

Objectives

Apprentices should be able to demonstrate an understanding of tools and methods required to implement security within computers and networks. Key areas are:

1. The ability to demonstrate a thorough knowledge of tools and methods employed to implement host based security for a range of threats.
2. A comprehensive knowledge of the technologies and techniques necessary for the defence and maintenance of networks and their hosts.
3. Understand the functionality and operation of security techniques as they apply to software and data.
4. A thorough understanding of the application, deployment and management of the security of networked systems and methods available to identify and reduce risk.

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 enrolled in the Level 4 Cyber Security Technologist apprenticeship programme requiring an understanding of Cyber Security Technology Building Blocks.

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 125 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 objectives 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 Providers

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. Host-based Security (20%, K2)

In this key topic, the apprentice should describe and explain the tools and methods commonly employed to protect hosts, application and system software and stored data from a range of threats, as well as the responsibilities of computer users in keeping their systems secure. Outcomes should include an ability to:

1.1 Describe computer and data authentication methods in current use.

1.2 Describe methods employed to protect and secure data held on the host. Indicative areas of study can include, but are not limited to:

- Types of authentication
- Access control
- Physical security
- TCP ports
- Disk encryption
- Checksums

1.3 Explain the importance of and the methods employed to keep the software environment healthy and up to date. Indicative areas of study can include, but are not limited to:

- Zero day attacks
- Operating system and application updates
- Antivirus updates

1.4 Describe the responsibilities of the user for PC protection, in keeping their PC and its data secure from threats. For example, but not limited to:

- Social engineering
- Software updates
- Password management
- Internet etiquette

2. Network-based Security (40%, K2)

In this key topic, the apprentice is required to identify and select appropriate technologies and techniques necessary for the defence of computer networks, their hosts and their users. Outcomes should include an ability to:

2.1 Describe the hardware components available for network protection and their purpose and demonstrate the ability to select the appropriate system for a given task. Indicative technologies can include, but are not limited to:

- Firewalls and DPI
- Application proxies
- IDS vs. IPS
- RADIUS
- AAA

2.2 Describe the policy based methods available for network protection and explain their purpose. For example, but not limited to:

- QoS
- Cross-domain components
- DMZ
- Gateways
- Routing
- Traffic prioritisation
- Anomaly & misuse detection

2.3 Describe methods available for the protection of data whist in transit and demonstrate the ability to select from a range of current technologies and appropriate methods for the protection of data as it crosses arbitrary networks. Indicative areas of study are secure Internet transaction technologies; including but not limited to:

- IPSec
- TLS
- SSH
- Negotiation
- Cryptography
- Key management

2.4 Describe the responsibilities of network administrators and approaches available for the management of security in the network. Apprentices should also explain the necessity for network and server configuration and maintenance, as well as available methods. Including but not limited to:

- Network segregation
- Security issues for common client & server configuration
- Performance management
- Staff training
- File and user permissions
- Password management

3. Application of Security for Software and Data (20% K3)

In this key topic, the apprentice will identify and select appropriate technologies and techniques necessary for the defence of software, applications and the data held on hosts. Outcomes should include an ability to:

3.1 Describe frameworks and processes available for secure application development and apply appropriate security processes to the software development lifecycle. Typical areas of study can include, but are not limited to:

- OWASP Top 10 awareness for web application development
- Common Weakness Enumeration guideline awareness for general software development
- National Cyber Security Centre (NCSC) guidelines
- Secure SDLC

3.2 Describe IDAM Tools and systems available for application and data protection, and how these can be applied to manage application security. For example, but not limited to:

- Identity management systems and protocols
- Tickets
- Tokens
- Session
- Multi factor authentication
- Access control
- Definitions (identity, authentication, authorisation, Bell-LaPadula model)

3.3 Describe application firewalls and reverse proxies and demonstrate the ability to select from a range of current technologies or appropriate tools to enhance the protection of data as it is captured and returned by applications. Indicative technologies can include, but are not limited to:

- Application sensors
- Application firewalls
- Proxies and reverse proxies
- Application level security logging and monitoring
- Log configuration

3.4 Describe database security mechanisms, including the responsibility of encryption in protecting user data; show the necessity for securing data at rest and describe different ways this can be done using database applications. For example, but not limited to:

- Field vs record based encryption
- SQL security
- Backup security
- Database access control

4. Management of Network Security and Risk in Networked Systems (20% K3)

In this key topic, the apprentice will select technologies and techniques necessary for the management of a secure computer system and describe risk mitigation techniques that can be applied at the host, network or application layer to secure computer systems. Outcomes should include an ability to:

4.1 Correctly apply risk mitigation techniques; such as, but not limited to:
- Threat modelling (example STRIDE)
- Security controls (SANS Top 20, NIST 800-53, GPG 13)

4.2 Apply security mechanisms as they relate to the CIA Triad; particularly, how to select security mechanisms to implement all three into a computer system. Indicative areas of study can include, but are not limited to:
- Confidentiality (select layers for encryption)
- Integrity (validating the integrity of data transmissions)
- Availability (load balancing, proxies, anti DDOS, WAF)

4.3 Explain accreditation and assurance processes that relate to the application of security technology. Apprentices will demonstrate the ability to apply supplier, software and component assurance and accreditation processes (first introduced in the Cyber Security Technologist, Knowledge Module 2 and described in sections 1 to 3 above). Indicative study can include, but is not limited to:
- Penetration testing
- Vulnerability assessment and threat intelligence
- ISMS and standards role in accreditation and supplier assurance (ISO27001, PCI DSS, common criteria, product assurance)
- Software code review (SAST, DAST, IAST, reviews)

4.4 Describe Security Technology Solutions in terms of their benefits and limitations and explain strengths, weakness and applicability of security technology as described in section 1 to 3 above. Typical areas of study can include, but are not limited to:
- Automation vs. manual validation of security
- Open source vs. closed source solutions
- On premises vs. off premises solutions (cloud based, private, hybrid and public)
- Iterative vs. Waterfall projects implication on security engineering

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. Host-based Security. (20%, K2)	8
2. Network-based Security. (40%, K2)	16
3. Application of Security for Software and Data. (20% K3)	8
4. Management of Network Security and Risk in Networked Systems. (20% K3)	8
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)	125 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