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

Version 3.0
March 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 Award in Security Technology Building Blocks

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	Mandatory Ofqual text added
Version 2.0 October 2019	Update to branding. Exam question balance also amended.
Version 3.0 March 2020	Full syllabus review

Introduction

This award is the fourth of the five knowledge modules that are applicable to the Technologist pathway for the Level 4 Cyber Security Technologist Apprenticeship. This module is all about cyber security technology components typically deployed in networks and systems to provide security functionality objectives.

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. Describe common types of security hardware and software which are used to protect systems (e.g. firewalls, encryption for data at rest, encryption for communication, IDS, IPS, IDAM tools, AV, web proxy, application firewalls, cross domain components, HSM, TPM, UTM).
2. Explain how each may be used to deliver risk mitigation or implement a security case.
3. Understand the benefits / limitations of each and taking into account the implicit assurance (including supplier assurance and considering the benefits and risks of open source options) of the component, describe any residual risks.

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

This qualification 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 award by attending a training course provided by a BCS accredited Training Provider. The estimated total qualification time for this award is 94 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 30-minute multiple-choice examination consisting of 20 questions. The examination is closed book (no materials can be taken into the examination room). The pass mark is 13/20 (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 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. Security Building Blocks (100%, K2)

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

1.1 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.

1.2 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.

1.3 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.

1.4 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.

1.5 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.

1.6 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.

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. Security Building Blocks.	20
Total	**20 Questions**

Format of Examination

Type	20 Question Multiple Choice.
Duration	30 Minutes. An additional 25% 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	13/20 (65%).
Calculators	Calculators cannot be used during this examination.
Total Qualification Time (TQT)	94 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

Title: Security Operations in Practice
Author: Mike Sheward
Publisher: BCS, The Chartered Institute for IT; 3rd edition
Publication Date: 29 Feb 2020
ISBN-13: 9781780175065