Making IT good for society

BCS Level 4 Award in Network (Cyber Intrusion Analyst) Syllabus 603/2892/7

Version 1.1 February 2018

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.

Making IT good for society

BCS Level 4 Award in Network (Cyber Intrusion Analyst)

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
V1.0	Document created.
V1.1	Edited title page and Contents page to include certification.

Introduction

This award is the first module of five knowledge modules that are applicable to the level 4 Cyber Intrusion Analyst apprenticeship. It covers the range of concepts, approaches and techniques that are applicable to networks, for which apprentices are required to demonstrate their knowledge and understanding.

Objectives

Apprentices should be able to demonstrate an understanding of modern computer networks. Key areas are:

1. Understands the 7 layer OSI model and UDP/TCP/IP network model.
2. Understands typical digital network architectures for LAN and WAN scenarios.
3. Understands difference between different kinds of networking equipment.
4. Understands virtual network techniques and the benefits of the different approaches.
5. Aware of IEEE 802 standards.
6. Understands typical approaches to implementation of VoIP.
7. Aware of network issues specific to wireless LAN and mobile cellular.
8. Aware of main security controls and appliances employed in digital networks.

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 award is relevant to anyone enrolled on the Level 4 Cyber Intrusion Analyst Apprenticeship programme.

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 118.5 hours.

Eligibility for the Examination

Individual employers will set the selection criteria, but this is likely to include 5 GCSEs (especially English, mathematics and a science or technology subject); other relevant qualifications and experience; or an aptitude test with a focus on IT skills.
Level 2 English and Maths will need to be achieved, if not already, prior to taking the endpoint assessment.

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 Training Providers

Each major subject heading in this syllabus is assigned an allocated time. The purpose of this is two-fold: first, 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; second, to guide the proportion of questions in the exam. Training providers 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 Network Security and Protocols (30%, K2)

In this topic area, the apprentice will describe and explain the common networks in use and their associated data formats and protocols. The successful apprentice should be able to:

1.1 Describe the components and equipment of a network.

- hubs;
- switches (L2 and L3);
- bridges;
- WAPs;
- routers;
- firewalls;
- proxy servers.

1.2 Explain the features of network protocols in widespread use on the Internet.

- HTTPS;
- HTTP;
- SMTP;
- SNMP;
- TCP;
- UDP;
- IP.

1.3 Summarise the main security controls and appliances employed in digital networks.

2 Layered Network Models (27.5%, K2)

In this topic area, the apprentice will be able to explain network layer models and then identify their differences. The successful apprentice should be able to:

2.1 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.

2.2 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.

2.3 Describe the typical approaches and components to implementing VoIP.

- terminal (user interface);
- gateway;
- gatekeeper;
- multipoint control unit (MCU).

3 Network Principles and Routing Protocols (15%, K2)

In this topic area, the apprentice will describe and explain network routing protocols. The successful apprentice should be able to:

3.1 Describe current network routing protocols in facilitating interoperability in network communications.
- RIPv1;
- RIPv2;
- RIPng;
- OSPF;
- OSPFv2;
- OSPFv3;
- EIGRP;
- EIGRP for IPv6.

3.2 Describe the differences between LAN and WAN scenarios.

4 Network Performance (7.5%, K2)

In this topic area, the apprentice will understand how network performance can be affected. The successful apprentice should be able to:

4.1 Identify the factors that affect network performance.
- bandwidth;
- number of users;
- contention.

5 Standards (2.5%, K2)

In this topic area, the apprentice will describe and explain the factors that affect network performance. The successful apprentice should be able to:

5.1 Summarise the key features of IEEE 802 standards.
- local area networks (LANs);
- metropolitan area networks (MANs).

6 Network addressing (17.5% K3)

In this topic area, the apprentice will learn the principles of network addresses. The successful apprentice should be able to:

6.1 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;
  - extended address space.

Levels of Knowledge / SFIA Levels

This syllabus 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 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. Network Security and Protocols	12
2. Layered Network Models	11
3. Network Principles and Routing Protocols	6
4. Network Performance	3
5. Standards	1
6. Network Addressing	7
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	Training from a BCS accredited training provider 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)	118.5 Hours, 67.5 GLH recommended.
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